بسم الله الرحمن الرحيم

الجامعة الإسلامية - غزة
عمادة الدراسات العليـــا
كليـــــــــة التجارة
قسـم إدارة الأعمـــال

متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة

إعداد الطالب:

صلاح عبد الحكيم المصري

تحت إشراف:

الدكتور/ عصام البحيصي – كلية التجارة

الدكتور/ توفيق برهوم – كلية تكنولوجيا المعلومات

قدمت هذه الدراسة استكمالاً لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال

2007 / 1428

قال الله تعالى:

"يَرْفَعِ ٱللَّهُ ٱلَّذِينَ ءَامَنُواْ مِنكُمْ وَٱلَّذِينَ أُوتُواْ العلم دَرَجَٰتٍ وَٱللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ (١١) "سورة المجادلة

صدق الله العظيم

ملخص الدراسة

هدفت هذه الدراسة إلى التعرف على متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة متمثلة في (تطوير البنية التحتية لمركز تكنولوجيا المعلومات، اهتمام الإدارة العليا لمركز تكنولوجيا المعلومات باستخدام التوقيع الإلكتروني، وجود المتطلبات القانونية والتشريعية لاستخدام التوقيع الإلكتروني ، اعتماد المراسلات الإلكترونية وسياسات حماية المعلومات الإلكترونية) ، وتهدف الدراسة إلى توضيح أهمية الحفاظ على أمن المعلومات واستخدام التقنية المتطورة في حماية الخصوصية خلال المراسلات الإلكترونية. حيث استخدم الباحث المنهج الوصفي التحليلي، حيث تكون مجتمع الدراسة من جميع موظفي مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، وقد تم الاعتماد على الاستبانة لجمع البيانات حيث تم توزيع 74 استبيان استجاب منهم 58 استبانة أي ما نسبته 78% من المجتمع الكلي للدراسة.

وقد خلصت الدراسة إلى أن تقنية التوقيع الإلكتروني لا تستخدم في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة ، وأن المعدات والبرمجيات الأمنية المستخدمة في مراكز تكنولوجيا المعلومات بحاجة إلى تحديث لتكون قادرة على حماية المعلومات الإلكترونية بكفاءة وأن موظفي مراكز تكنولوجيا المعلومات لديهم قصور لمفهوم التوقيع الإلكتروني.

وقد خرجت الدراسة بعدة توصيات أهمها: أن إدارة الجامعات الفلسطينية بحاجة لاعتماد المراسلات الإلكترونية الرسمية باستخدام التوقيع الإلكتروني، تحديث المعدات الأمنية وتطوير برمجيات أمن المعلومات المستخدمة حالياً في مراكز تكنولوجيا المعلومات، و تخصيص موازنة سنوية خاصة بأمن المعلومات وتدريب موظفي مراكز تكنولوجيا المعلومات في مجال أمن المعلومات، وضع وتطوير سياسات خاصة بأمن المعلومات وباستخدام التوقيع الإلكتروني بصورة مستمرة في مراكز تكنولوجيا المعلومات.

Abstract

This study aimed to identify the acquisition of the use of digital signature in the management of information technology centers (ICT) in the Palestinian universities in the Gaza Strip represented in the (development of the infrastructure of the ICT, the attention of senior management of the ICT using digital signature, a legal and legislative requirements for the use of digital signature, adoption electronic correspondence and policies to protect electronic information), the study aims to clarify the importance of preserving the security of information and the use of technologically advanced equipment to protect privacy through electronic correspondence.

The researcher used descriptive analytical approach, where a study of all the staff of information technology centers in the Palestinian universities in the Gaza Strip, has been relying on results of the data collection by a questionnaire distributed 75; respondents were 58 which mean 77%.

The study concluded that the digital signature technology is not used in the information technology centers at Palestinian universities in the Gaza Strip, and security hardware and software used in the information technology centers need to be updated to be able to protect electronic information efficiently and staff information technology centers have limitations of the concept of electronic signature.

The study came out several recommendations, including: the administrations of the Palestinian universities need to adopt electronic correspondence using official electronic signature, updating security equipment and the development of information security software currently used in the information technology centers, and special annual budget allocation to information security and training the staff of information technology centers in the area of information security, the formulation and development of policies for the security of information and using electronic signature constantly in the information technology centers.

الإهـداء

إلى روح والدي رحمه الله

إلى والدتي العزيزة التي حثتني دائماً على الدراسة وإلى زوجتي الغالية التي شجعتني كثيراً على الدراسة وقدمت لي كل عون

إلى أرواح الشهداء

إلى من يحب النجاح والتوفيق ويرجوه لي

إلى طلبة العلم في كل مكان

أهدي جهدي المتواضع لهم جميعاً

الشكر و التقدير

أتوجه بالشكر لله سبحانه و تعالى الذي ارتضى أن يكون شكر الناس شكراً له . . . كما أتوجه بالشكر والتقدير لأعز وأغلى الناس والدتي العزيزة لدعائها لي في إنهاء هذة الدراسة، كما أتوجه بالشكر والتقدير لزوجتي الغالية لمساندتها لي لإنجاح وإتمام هذه الدراسة جزاهما الله عني خير الجزاء . .

كذلك أتقدم بجزيل الشكر وعظيم الامتنان إلى أساتذتي: الدكتور عصام البحيصي و الدكتور توفيق برهوم على نصائحهما السديدة و تفضلهما بالإشراف على هذه الدراسة جزاهما الله كل خير.

كما أشكر الاستاذ الدكتور/ يوسف عاشور، و الدكتور/ رشدي وادي لتفضلهما بقبول مناقشة هذه الرسالة.

وكذلك أتقدم بشكري للجامعة الإسلاميةالتي اعمل بها وتمنحني بهذة الدراسة الدرجة العلمية الثانية إن شاء الله . . . .

قائمة المحتويات

قائمة الجداول

مصطلحات الدراسة

#	المصطلح	التعريف
1	**authentication**	الموثوقية او الإثبات: وهى عملية التحقق من هوية المرسل
2	**authorization**	ترخيص أو تخويل : وتعتبر جزء من نظام التشغيل لحماية مصادر الحاسوب من الدخول للأشخاص الغير مسموح لهم بذلك
3	**password /username**	اسم المستخدم: هو عبارة عن حساب خاص مع كلمة مرور يمكن بواسطتة الدخول على: جهاز الكمبيوتر ، أو برنامج ، أو موقع إنترنت أو ... إلخ
4	**VPN**	Virtual private networks(شبكات الحاسوب الوهمية): هى عبارة عن شبكات حاسوب ناتجة عن عملية إعدادات معيتة باستخدام برمجيات خاصة.
5	**Biometrics Signature**	هو توقيع يتم باستخدام الخواص الذاتية للإنسان مثل بصمة الأصبع أو قزحية العين.
6	**Digital Certificates- DC**	الشهادات الرقمية: هى عبارة عن رسالة تحتوي على معلومات مرتبطة بهوية المرسل و بالمؤسسة التابع لها، فهي تؤكد مصداقية المفتاح العام أو بملكية موقع على الإنترنت.
7	**Certificate Authorities -CA**	هيئة إصدار الشهادات: هى مؤسسة رسمسة معتمدة لإصدار الشهادات الرقمية
8	**Smart Cards**	البطاقات الذكية: هي عبارة عن كرت بحجم المحفظة يحتوي على دائرة متكاملة لمعالجة المعلومات.
	SIM Cards	هي عبارة عن شريحة إلكترونية يتم تركيبها في جهاز المحمول محتوية على معلومات خاصة بالمستخدم.
9	**Trusted third Party**	جهة ثالثة محايدة لتصديق الشهادات الرقمية

10	**Asymmetric Cryptography**	التشفير اللامتماثل ، هو عبارة عن تشفير زوج من المفاتيح الغير متماثلين تستخدم لتشفير ولفك تشفير الرسالة لتكون أمنة.
11	**Symmetric Cryptography**	التشفير المتماثل : هو التشفير الذي يستخدم نفس المفتاح من أجل التشفير و فك التشفير
12	**Web Server**	ويب سيرفر أو خادم الويب وهو جهاز مخصص لوضع وتشغيل موقع الإنترنت الخاص بالمؤسسة .
13	**Keys**	المفاتيح: هى عبارة عن زوج من المفاتيح تستخدم لإنشاء التوقيع الإلكتروني، ولكل توقيع مفتاح عام ومفتاح خاص
14	**Public Key**	المفتاح العام: هو مفتاح متوفر لدى العامة يستخدمونه للتأكد من صحة توقيع الرسالة الموقعة بالمفتاح الخاص بالمرسل.
15	**Private key**	المفتاح الخاص: هو عبارة عن كود خاص يستخدم من قبل شخص معين وبكلمة مرور للمراسلات الإلكترونية ليتمكن المستقبل من التحقق من عدم حدوث أي تغييرعلى الرسالة منذ توقيعها من قبل مرسلها.
16	**Cryptosystems**	أنظمة تشفير: هي أنظمة تعمل على تشفير البيانات بحيث لا يمكن قراءتها
17	**Encryption**	التشفير: هى عبارة عن عملية تحويل البيانات النصية إلى شكل رموز وأرقام لا يمكن قراءتها بدون عملية عكسية لفك التشفير
18	**Public-key cryptography**	تشفير المفتاح العام: التقنية المستخدمة لإنشاء هوية رقمية digital IDs، فعند التوقيع باستخدام الهوية، فإنك بذلك تصدر مفتاحين "المفتاح العام" ويكون مظهراً في الشهادة الرقمية الخاصة بك، والمفتاح الخاص ويكون لدى المرسل فقط.
19	**Directory Service**	دليل الخدمة: هي عبارة عن قاعدة بيانات تبين مدى صـلاحية الـشهادة الرقمية منأنها سارية المفعول أم أنها ملغية.
20	**Hacker**	مخترق الحاسوب: هو عبارة عن شخص يحاول اقتحام أجهزة الحاسوب

قائمة الإختصارات

#	المصطلح	البيان
1	**PIN**	Personal Identification Number
2	**PKI**	Public Key Infrastructure
3	**HTTP**	hypertext transfer protocol
4	**B2B**	Business to Business
5	**CRL**	Certificates Rejected list
6	**PDA**	Personal digital assistant
7	**CA**	Certificate Authority
8	**E-Sign Act**	Electronic Signatures in Global and National Commerce

قائمة الملاحق

الفصل الأول

الإطار العام للدراسة

أولاً: مقدمة

ثانياً: مشكلة الدراسة.

ثالثاً: أسئلة الدراسة.

رابعاً: فرضيات الدراسة

خامساً: أهمية الدراسة

سادساً: أهداف الدراسة

سابعاً: متغيرات الدراسة

ثامناً: منهجية الدراسة وجمع البيانات

تاسعاً: هيكل الدراسة

عاشراً: الدراسات السابقة

المقدمة:

أصبحت المعلومات هي سمة العصر الذي نعيشه حتى أن الـبعض أطلـق عليـه عـصر المعلومات، وتكتسب المعلومات أهميتها من إنتشارها وقيمتها وتبادلها بين البشر ولا يمكـن أن يتم تبادل هذة المعلومات دون وجود شبكات نقل المعلومات التي أدت إلـى سـرعة وسـهولة الحصول على المعلومة أو نشرها بغض النظر عن بعدها الجغرافي وبمختلف المجالات العلمية، الإنسانية، الثقافية، البحثية و. . .إلخ، المومني (2003).

لكن رغم هذا التطور السريع في شبكات الإتصالات والمعلوماتية خاصة بعد ظهور الإنترنـت وما تتعرض له شبكات المعلومات من إختراقات أو التنـصت علـى المعلومـات الإلكترونيـة وكشفها، خاصة تلك التي تهم مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية بشكل خاص وما تحمله من مخاطر مادية أو معنوية في حال كشف أو سرقة أو تحريف المعلومات الخاصـة بها، فإنه لا بد من حماية هذة المعلومات والمحافظة عليها من أي اختراقات عند تنقلهـا عبـر الشبكات، فكانت هناك الحاجة للتوقيع الإلكتروني لحماية هذة البيانات، المومني (2003).

فالتوقيع الإلكتروني يهدف إلى الحد من مشكلة الأمن والخصوصية على شبكة الإنترنت، فاللجوء إلى التوقيع الإلكتروني يعمل على توفير مستوى متقـدم مـن الأمـن والخـصوصية للمتعاملين عبر شبكة الإنترنت وشبكة الحاسوب الداخلية للمؤسسات، فالأمن يشغل حيزاً كبيـراً من مستخدمي شبكة الإنترنت سواء كانوا مشترين أو مزودين، فالإنترنت مجال مفتـوح وغيـر مسيطر عليها من قبل جهة محددة، فالإتصال عبر الإنترنت غير آمن، لذلك إنتقال البيانات عبر الإنترنت يزيد من التوقعات في اعتراض أو تحريف البيانات، فالمعلومات الحساسة يمكن قرائتها من قبل جهات غير مخول لهم الإطلاع عليها، كذلك فالإتفاقيات المبرمـة مفتـرض أن تكـون ملزمة لطرفي العقد وأن لا تكون محل خلاف لطرفي العقد فيما بعد، لذلك فالتوقيع الإلكترونـي هى طريقة لتوقيع الوثائق الإلكترونية، ولمساعدة مستقبل الرسالة من التحقق من مصدر الرسالة ومن هوية المرسل، ومن أن محتوى الرسالة لم يجري عليه أي تغيير أثناء ارسالها بعد توقيـع المرسل عليها، فهى تقنية تمنع المرسل من انكار توقيعه. لذلك هناك أربعة احتياجات لا بد مـن تحقيقها لإبرام العقود الإلكترونية عبـر الإنترنـت وهـي: المـصداقية (Authentication)، والخصوصية (Confidentiality or Privacy) ، والتكاملية (Integrity)، وعـدم الإنكـار (non- repudation)، موقع (teletrust.de)، و لأجل ذلك يستخدم التوقيع الإلكتروني لتوفير ثلاثة خدمات أمنية في غاية الأهمية وهي: المصداقية وعدم كشف البيانـات وعـدم تحريـف البيانات وعدم الإنكار، Hassler (1999).

مشكلة الدراسة:

جاءت هذه الدراسة لإلقاء الضوء على متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وإلى عدم وجود نموذج في هـذة المراكز لإستخدام التوقيع الإلكتروني.

و تبرز المشكلة في التساؤل التالي :

" ما متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعـات الفلسطينية في قطاع غزة".

أسئلة الدراسة:

1. ما مدى اهتمام موظفي مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة باستخدام التوقيع الالكتروني ؟

2. ما مدى تطوير البنية التحتية في مراكز تكنولوجيا المعلومات لاستخدام التوقيع الإلكترونـي في الجامعات الفلسطينية في قطاع غزة ؟

3. ما المتطلبات القانونية والتشريعية لاستخدام التوقيع الالكتروني؟

4. هل المراسلات الالكترونية هي المراسلات الرسمية المعتمـدة فـي مراكـز تكنولوجيـا المعلومات ؟

5. هل يوجد سياسات لحماية المعلومات الإلكترونية؟

6. هل يوجد نموذج لإستخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة ؟

فرضيات الدراسة:

1. لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين تطوير البنية التحتية لمراكز تكنولوجيا المعلومات.

2. لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني.

3. لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين وجود المتطلبات القانونية والتشريعية لاستخدامه.

4. لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اعتماد المراسلات الإلكترونية.

5. لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين السياسات المستخدمة حالياً.

أهمية الدراسة:

في ضوء إختراقات المعلومات الإلكترونية من قبل مخترقي أجهزة الحاسوب (Hackers)، برزت الحاجة لتوفير المزيد من الحماية والخصوصية لهذة المعلومات للوقاية من مخاطر تحريفها خاصة في حالة المراسلات الإلكترونية، وهذا شكل دافعاً قوياً لإيجاد وسائل حماية أكثر فاعلية للمحافظة على تكاملية البيانات الإلكترونية لمؤسسات التعليم العالي والتي يفترض أن تكون مثال يهتدي به للمؤسسات الأخرى لحماية المعلومات الإلكترونية. وتنبثق أهمية هذة الدراسة من حيث:

- أصالتها: حيث أنها تعتبر الدراسة الأولى من نوعها (فيما اطلعت) التي تتطرق إلى بحث هذا الموضوع في فلسطين.

- تعتبر هذة الدراسة كمصدر معلومات تستفيد منها المؤسسات والمراكز ذات العلاقـة التـي ترغب في تطوير سياساتها لحماية المعلومات الإلكترونية.
- يمكن اعتبار هذه الدراسة كمصدر للباحثين والدارسين باللغة العربية الذين يودون التعـرف أكثرعلى تقنية التوقيع الإلكتروني وفعاليته وكيفية تطبيقه.

أهداف الدراسة:

1- التعرف على متطلبات استخدام التوقيع الإلكتروني في مراكز تكنولوجيـا المعلومـات فـي الجامعات الفلسطينية في قطاع غزة.
2- التعرف على الأسباب التي تؤدي إلى عزوف مراكز تكنولوجيا المعلومات في الجامعـات الفلسطينية في قطاع غزة عن استخدام التوقيع الإلكتروني .
3- تصميم نموذج تطبيقي لإستخدام التوقيع الإلكتروني من قبل مـوظفي مراكـز تكنولوجيـا المعلومات في الجامعات الفلسطينية في قطاع غزة.
4- الخروج بتوصيات وما مدى فعاليتها في تطبيقها على أحد الجامعات الفلسطينية فـي قطـاع غزة والتي من شانها أن تبلور الحلول المناسبة لهذه المشكلة.

متغيرات الدراسة

المتغير التابع: متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة.

المتغيرات المستقلة:

- تطوير البنية التحتية لإستخدام تقنية التوقيع الإلكتروني
- اهتمام الإدارة العليا باستخدام تقنية التوقيع الإلكتروني.
- المتطلبات القانونية والتشريعية لاستخدام التوقيع الالكتروني.
- اعتماد المراسلات الإلكترونية داخل الجامعات.
- توفير سياسات لحماية المعلومات الإلكترونية في مراكز تكنولوجيا المعلومات.

منهجية الدراسة:

تم استخدام المنهج الوصفي التحليلي في إجراء الدراسة وهو الأنسب في دراسة الظـاهرة موضع البحث.

منهجية جمع البيانات:

استخدمت المصادر الثانوية والأولية في الدراسة، وتتكون المصادر الثانوية من الكتـب والمجلات العلمية المتخصصة ومواقع الإنترنت وخاصة رسائل علمية سابقة عالجت ظـاهرة متطلبات استخدام التوقيع الإلكتروني، أما استخدام المصادر الأولية فمن خلال الاستبانة.

هيكل الدراسة

تتكون هذة الدراسة من سبعة فصول وهي كالتالي:

الفصل الأول: الإطار العام للدراسة(مقدمة عامة للدراسة، مشكلة البحث والفروض والأهداف والأهمية والدراسات السابقة).

الفصل الثاني: (الإطار النظري).

- مفهوم التوقيع الإلكتروني وآلية عمله
- البنية التحتية للمفتاح العام
- الشهادات الرقمية
- سلطة منح الشهادات الرقمية
- سياسات حماية المعلومات
- حجية التوقيع الإلكتروني

الفصل الثالث: واقع مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة.

الفصل الرابع: اجراءات الدراسة

الفصل الخامس: تحليل وتفسير فقرات الدراسة واختبار الفرضيات.

الفصل السادس: نموذج تطبيق التوقيع الإلكتروني

الفصل السابع : النتائج والتوصيات.

الدراسات السابقة

1. دراسة **Wilson (1998)**

توضح الدراسة إلى كم من التواقيع الإلكترونية والمعلومات عبـر الإنترنـت تحققـت بالتوثيق الإلكتروني حيث تستخدم حالياً أوراق اعتماد إلكترونية لأصحاب المـؤهلات المهنيـة (أطباء، محامين، محاسبين، ...إلخ) وتوصل الباحث إلى أن:

- الكثير من العمل سينجز إلكترونياً دون استخدام المعاملات الورقية.
- وضوح الوضع القانوني يعمل على انجاز العقود عبر الإنترنت بشكل فعلي دون الـضرورة إلى الورق او التوقيع علية.
- أمـن الوثـائق الإلكترونيـة تـشتمل علـى: التكامليـة (Integrity) والموثوقيـة (Authentication) والخصوصية (Privacy) وهى ذات فعالية أعلى من المعاملات الورقية.

2. دراسة **Borasky (1999)**

وتهدف الدراسة إلى التركيز على التوقيع الإلكتروني كإثبات قـانوني للإتفاقيـات عبـر البريد الإلكتروني .

وخلصت الدراسة إلى أن التوقيع الإلكتروني قيد الإستخدام حالياً حول العـالم وسـوف يستخدم بشكل كبير في حال تعزيز التكنولوجيا وتفنيد طرق وأساليب مخترقي أنظمة الحواسيب ونتيجة لعدم تشريع التوقيع الإلكتروني أدى ذلك إلى تأخر إستخدامه. وهناك مزايـا واضـحة للتوقيع الإلكتروني كالرعاية الصحية، مالية، تعليم، ..إلخ فإنه سيكون هناك بعض من المستفيدين المحتملين حيث تَبدو هناك عقباتَ حاليةَ تَمنع الإسـتعمالَ الواسـع الإنتـشار علـى مـستوى المستهلكِ. ومع ذلك فإن السوق العالمي والمنافع المرافَقَة للتجارة الإلكترونية وصفقات عبـر الإنترنت تتُضاعفُ بنسبة كبيرة. و إنه إفتراض آمن أن تقنيةِ التوقيع الإلكتروني ستَحتفظ بتقدمها وفي نفس الوقت سيبقى القلم في متناول اليد.

3. دراسة **Godwin (2001)**

تبين الدراسة أن عدم الثقة بتكنولوجيا المعلومات عبر الإنترنت ليس فقط نتيجـة قيمـة الامن المفقودة ولكن أيضاً نتيجة عدم الثقة بمجتمع المعلومات، فالخصوصية هي أحد الأسـباب التي أدت إلى عزوف الزبائن عن الشراء عبر الإنترنت وخلصت الدراسة إلى أن:

- المخاوف الرئيسية التي يواجهها المشترين عبر الإنترنت هي الخـصوصية والأمـن أثنـاء التسوق عبر الإنترنت.
- موظفي المؤسسة يفضلون أن يكون للمؤسسة سياسات واضحة لإستخدامات الإنترنت والبريد الإلكتروني وتوضيح هذة السياسات للموظفين.
- إن وجود مثل هذة السياسات وتنبيه الموظفين إليها سوف يؤدي إلـى خفـض المـسؤوليات والمخاطر الأمنية للشركة.
- تحمل المسؤولية في توعية مستخدمي تكنولوجيا المعلومات وتوفير المعـدات والبرمجيـات الضرورية لذلك سوف يؤدي إلى تحسين مستوى الأمن والخصوصية.

4. دراسة **David (2001)**

بينت الدراسة مزايا وجود الإنترانت في داخل المؤسسة لتحسين عملية الإتـصال بـين موظفي وأقسام المؤسسة والحصول على المعلومات الخاصة بالمؤسسة بكل سهولة، حيث أنهـا تناقش المنافع والمخاوف والتحديات نتيجة وجود شبكة الإنترانت فـي المؤسـسة وتوصـلت الدراسة إلى أن وجود الإنترنت في المؤسسة يزيد من قيمة المعلومات وتدفقها داخل المؤسـسة مما يؤدي إلى الوصول إلى مصادر المعلومات المتنوعة في المؤسسة بكل سهولة وفي النتيجـة توفير في الوقت والجهد والتكاليف بالنسبة للمؤسسة.

5. دراسة **Kuechler (2002)**

تهدف الدراسة إلى الإجابة على السؤال" لماذا أصبح التوقيع الإلكتروني ضـروري للتجـارة الإلكترونية" وخلصت الدراسة بتوصيات منها:

- تحديد أولاً الإحتياجات لتطبيق تقنية التوقيع الإلكتروني المعقدة والمكلفة وهل لدى الـشركة الإمكانيات لتحمل الأعطال الهامة إذا تعرضت للكشف أو سوء الإستخدام.
- أن يقوم خبراء مختصين بالأمن باقتراح آلية كطريق وحيد لتحديـد الإلتزامـات لإسـتخدام التوقيع الإلكتروني في المستقبل القريب.
- التأكد من أن أي شركاء في أي تجارة الإلكترونية قد وافقوا بشكل رسمي على قبول التواقيع الإلكترونية كملزمة قانونية.
- البحث في إجراءات أمن كلٍ من جهة إصدار الشهادات الرقمية الخاصـة بـك وبالـشركاء التجاريون.

6. دراسة **Gabor (2004)**

بينت الدراسة مفهوم التوقيع وأنواع التواقيع الإلكترونية، وكذلك استخدامات وخصائص التوقيع الإلكتروني، حيث بينت أن:

- التوقيع الرقمي Digital Signature يعني تعريف إلكترونيElectronic Identifier أُنشئ بواسطة الحاسوب، بقصد استخدامه من قبل أفراد ليمتلك نفس القوة ونفـس التـأثير كاسـتخدام التوقيع التقليدي، وهو عبارة عن خوارزمية حاسوبية (computer algorithm) للتحقق بـين أجهزة الحاسوب من هوية المرسل والمستقبل والإثبات شرعاً من وجود هويـة الموقـع علـى المستند.

وبينت الدراسة استخدامات التوقيع الإلكتروني على النحو التالي:

أولاً: في حال الإتصال المكتوب مع الأخرين فإن استخدام التوقيع الإلكتروني سوف يمتلك نفس القوة والتأثير كالتوقيع التقليدي إذا فقط اشتمل على الخصائص التالية:

1. يكون وحيداً للشخص الذي يستخدمه It is unique to the person using it.
2. يكون قادراً على التحقق من هوية المرسل.
3. تحت السيطرة الوحيدة للشخص الذي يستخدمه
4. أن يكون مرتبطاً بالمستند تماماً بحيث أنه في حالة تحريف المـستند يكـون التوقيـع الإلكتروني باطلاً.

ثانياً: استخدام أو قبول التوقيع الإلكتروني سيكون حسب اختيار الأفراد .

ثالثاً: التوقيع الإلكتروني يستخدم طبقاً للقانون الخاص به.

7. دراسة **Edward (2004)**

وتهدف الدراسة إلى أهمية استبدال التوقيع التقليدي بالتوقيع الإلكترونـي فـي التجـارة الإلكترونية، وخلصت الدراسة إلى أن :

- العقود الإلكترونية أصبحت وبشكل متسارع بديلاً عن العقود الورقية وأنها سـوف تنتـشر أكثر في حالة أن شعر المستخدم بالأمان في استخدامها.
- القانون مع الوقت سوف يدعم التوجه إلى إعتماد التوقيع الإلكتروني.
- تشريع التوقيع الإلكتروني مهم لأنه سوف يكون البوصلة في صناعة التجارة الإلكترونية.

8. دراسة **Rodney (2004)**

بينت الدراسة أن المؤسسة تضع السياسات الخاصة بتكنولوجيا المعلومات طبقاً لاحتياجات العمل الداخلية بحيث أن تكون هذة السياسات متوافقة مع القانون العـام، وأن علـى الجامعـات والكليات وضع إطار عام لسياسات أمن المعلومات لتأخـذ بالحـسبان الاعتبـارات القانونيـة والأخلاقية والقيم الأكاديمية.

إن على المؤسسة أن تقدير المخاطر الأمنية و أن تضع برامج لحمايـة أمـن المعلومـات الإلكترونية لديها مثل المعلومات المالية والصحية، ويجب عليها أن تعمل على صـد الهجمـات الخارجية التي يمكن أن تتعرض لها أنظمة المعلومات في المؤسسة والوقاية من هذة الهجمـات، لذلك فإن على الجامعات والكليات أن تقوم بتطبيق الحماية لهذة المعلومات والحفاظ عليهـا دون الحاجة إلى قانون أو تشريع لتطبيق هذة الحماية داخل المؤسسة.

9. دراسة **Thomas (2006)**

وتهدف الدراسة إلى مدى تأثير الإدارة العليا للمؤسسة لدعم الثقافة الأمنية في المؤسسة ومدي تنفيذ السياسات الأمنية فيها وقد خلصت نتائج الدراسة إلى أن:

- دعم الإدارة العليا له تأثير ايجابي على ثقافة أمن المعلومات وتطبيق السياسات الخاصة بهـا وفي حالة عدم وجود دعم حقيقي لأمن المعلومات في المؤسسة من الإدارة العليا فإن برامج أمن المعلومات في المؤسسة ستفشل.
- في ظل عدم تأييد الإدارة العليا لأمن المعلومات في المؤسسة برغم من توفر التقنيات الأمنية المتطورة فيها فإنها لن تستطيع حماية المعلومات الداخلية للمؤسسة.
- انخفاض تأثير الإدارة العليا للمحافظة على أمن المعلومات سيؤدي إلى ضعف المستوى فـي تطبيق سياسات أمن المعلومات في المؤسسة.

10. دراسة **Shalhoub (2006)**

وتهدف الدراسة إلى أن إفتقار الثقة في المعاملات الإلكترونية هو أحد الأسباب الرئيسة في انخفاض التجارة الإلكترونية خاصة في الدول النامية مثل دول مجلس التعـاون الخليجـي، وخلصت الدراسة إلى أنه لزيادة الثقة في المعاملات الإلكترونية قامت بعـض الـشركات فـي مجلس التعاون الخليجي إلي:

- تطوير سياسات الخصوصية لمواقع الإنترنت الخاصة بها ونشرها على موقع الـشركة لبيان مدى حرص الشركة على خصوصية معلومات الزبائن .

- على جميع الشركات أن تقوم بتطوير السياسات الأمنية التي تتضمن جميع العناصر الأساسية الخاصة بتطبيق هذة السياسات.
- فشل سياسات أمن المعلومات أدى إلى عدم ثقة الزبائن بمواقع الشركات عبر الإنترنت.

11. دراسة **Kwo-Shing Hong (2006)**

الهدف من الدراسة هو معرفة أو تحديد العناصر الرئيسية في المؤسسة لبناء سياسات أمن المعلومات وما إذا كانت هذة السياسات قادرة لرفع مستوى الأمن في المؤسسة، وخلصت الدراسة إلى ان حجم قسم أنظمة المعلومات الإدارية يعتبر مؤشر على أن المؤسسة تدرك قيمة أنظمة المعلومات الإدارية وبالتالي كلما كان قسم أنظمة المعلومات الإدارية كبيراً فهذا مؤشر على أن هناك إمكانيو كبيرة لبناء سياسات أمن المعلومات في المؤسسة.

12. دراسة **Christopher (2007)**

وبينت الدراسة أن معاملات وإجراءات الجامعة تُنجز على نحو متزايد عبر الإنترنت وبشكل مباشر مثل: حصول الطلبة على المعلومات التعليمية الخاصة بهم، التسجيل الفصلي، المساعدات المالية، برامج قروض الطلبة، تلقي معلومات عن صرف المساعدات المالية عبر الإنترنت،...إلخ، حيث أن هناك إمكانية استخدام الكمبيالة الإلكترونية والتوقيع الإلكتروني بدلاً من المستند الورقي والتوقيع التقليدي. كلّ هذه الإجراءات خاضعة لقانون التواقيع الإلكترونية الإتحادية بفعل التجارة الإلكترونية العالمية والوطنية (Electronic Signatures in Global and National Commerce – ESIGN Act. , E-Sign Act.) لذا نظام المؤسسات يجب أن يضمن الإلتزام بمتطلبات القانون الفدرالي لكل الإجراءات التي تستخدم توقيعاً إلكترونياً حيث أن الـ E-Sign Act. تهدف إلى اقرار استخدام التواقيع الإلكترونية والعقود الإلكترونية بمنحها نفس الفعالية القانونية كما لو كانت بالشكل الورقي.

وتوصلت الدراسة إلى أن:

- ♦ المؤسسات التعليمية كنظام، تسعى لانجاز معاملات للطلبة وللموظفين عبر الإنترنت، فإنه يجب العمل سوياً لضمان استمرارية عمل تلك الأنظمة عبر الإنترنت ليتيح للمستخدمين الإشعارات والخيارات المطلوبة .
- ♦ التوقيع الإلكتروني يكون له أثر بالنسبة لنظام المؤسسات لإستمرارية تقييم الأساليب لجعل المعاملات أكثر أمناً عبر الإنترنت، بحيث أن المؤسسات تضمن تبني أنظمة التوقيع الإلكتروني في حالة توفر البنية التحتية للتوقيع الإلكتروني وتقلل من التكاليف.

13. دراسة **Whitaker (2007)**

مع ظهور التجارة الإلكترونية فإن التواقيع التقليدية سوف يستغنى عنها في ظل تعـاظم المبيعات عبر الانترنت، وبالتالي سوف يحل التوقيع الإلكتروني محل التوقيع القليدي، لذلك على الجامعة التي ترغب في استخدام السجلات الإلكترونية والتوقيع الإلكتروني أن تعمل على تهيئة بيئة العمل لإعتماد التوقيع الإلكتروني والسجلات الإلكترونية التي سوف دائمـاً تكـون محـل إهتمام، بخلاف الإعتماد على القانون فقط.

التعليق على الدراسات السابقة:

من خلال الدراسات السابقة فقد تبين التالي:

- لم يعثر الباحث على أي دراسة محلية أوعربية تتعلق باستخدام تقنية التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات وهذا يدل على أن هذة التقنية لا تستخدام في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة ومن هنا تكمن أهمية الدراسة الحالية.
- استفاد الباحث من الدراسات السابقة في أهمية وضرورة استخدام التوقيع الإلكتروني في المراسلات الإلكترونية في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية بشكل خاص وفي مراسلات إدارة الجامعات بشكل عام، كذلك على أهمية المحافظة على أمن وخصوصية المراسلات الإلكترونية خصوصاً وأمن المعلومات عموماً.
- لإستخدام التوقيع الإلكتروني في المراسلات الخارجية لمراكز تكنولوجيا المعلومات فإن ذلك يتطلب تشريع خاص بالتوقيع الإلكتروني من قبل المجلس التشريعي لإعتماده في مناطق السلطة الفلسطينية وهذة تعتبر من المتطلبات الضرورية للتوقيع الإلكتروني.

وقد توصلت بعض الدراسات إلى أهمية المحافظة على أمن ا لمعلومات في المؤسسات مثل الدراسات التالية:

دراسةshalhoub (2006)، ودراسة Thomas (2006)، ودراسة Rodney (2004)، ودراسات أخرى خلصت إلى ضرورة تشريع التوقيع الإلكتروني مثل الدراسات :

دراسة Gabor Moroc (2004) ، ودراسة Kuechler (2002).

وهناك دراسات جمعت بين عنصرين من بين ثلاث عناصر للأهمية(اتساع انتشار التوقيع الإلكتروني، أمن المعلومات، وتشريع التوقيع الإلكتروني) وخلصت أن التوقيع الإلكتروني سيكون أكثر إنتشاراً من التوقيع القليدي، أي أنه سيكون بديلاً عن التوقيع التقليدي مستقبلاً في ظل تعاظم المبيعات عبر التجارة الإلكترونية والمحافظة على أمن المراسلات الإلكترونية حيث أن المؤسسات تتجه لانجاز أعمالها وخدماتها إلكترونياً مع ضرورة تشريع التوقيع الإلكتروني مثل الدراسات التالية:

دراسة Christopher (2007)، ودراسة Edward (2004)، ودراسة Borasky (1999)، ودراسة Stephen(1998) .

وهناك دراستين هما: دراسة Christopher (2007)، ودراسة Whitaker (2007) تتفقان مع الدراسة قيد البحث حيث ان الجامعات تعمل على تقديم الخدمات الخاصة بالطلبة والمدرسين

عبر الإنترنت كذلك العمل على انجاز ممارسات العمل إلكترونياً وبشكل أمن، حيث أن هنالك تطابق في البيئة التعليمية مع هذة الدراسات للتحول إلى بيئة إلكترونية لتكون حافزاً للتوجه إلى بيئة تكنولوجية.

لكن الباحث يختلف مع الدراستين في :

أولاً: لإستخدام التوقيع الإلكتروني لا بد من توفير التشريع القانوني لتبادل المراسلات الإلكترونية فالدراسة الحالية تدرس في البيئة الداخلية لمراكز تكنولوجيا المعلومات في الجامعات الفلسطينية حيث أن هيئة تصديق الشهادات تكون جهة داخلية Certificate Authority -CA وبالتالي لا تحتاج إلى تشريع قانون خاص بالتوقيع الإلكتروني وإنما يحتاج إلى إعتماده من قبل إدارة الجامعة بينما في الدراسات السابقة فإن هيئة تصديق الشهادات CA تكون جهة خارجية نتيجة تبادل المراسلات الإلكترونية مع مؤسسات خارجية وبالتالي فهى بحاجة إلى تشريع قانون لذلك، فالتوقيع الإلكتروني يحتاج إلى تشريع قانون في مجال التجارة الإلكترونية أو المراسلات الإلكترونية الخارجية بين مراكز تكنولوجيا المعلومات والمؤسسات الخارجية.

ثانياً: بينت الدراسات السابقة أن تقديم الخدمات للطلبة باستخدام الـ PIN/Password عبر الإنترنت وكذلك بالنسبة للمدرسين لإدخال الدرجات يعتبران ذلك توقيعاً إلكترونياً، وهذا لا يتفق مع المفهوم العلمي لتقنية التوقيع الإلكتروني الذي يقصده الباحث لفقدة عناصر التوقيع الإلكتروني وهي(المفتاح العام، المفتاح الخاص، الشهادات الرقمية) وهذا ما يفتقده الـ PIN/Password أو اسم المستخدم وكلمة المرور الخاصة بالمدرس لإدخال الدرجات لأنه لا يمكن التحقق من هوية مدخل اسم المستخدم وكلمة المرور حيث يمكن استخدامهما بطريقة غير شرعية من قبل أشخاص غير مخولين بذلك وهذا لا يتفق مع تقنية التوقيع الإلكتروني.

❖ أوجه الإتفاق والإختلاف بين الدراسة الحالية والدراسات السابقة:

أولاً: اتفقت الدراسة الحالية مع الدراسات السابقة بالنقاط التالية:

1. بيان أهمية تقنية التوقيع الإلكتروني في المحافظة على امن المراسلات الإلكترونية.
2. ضرورة تطبيق واستخدام التوقيع الإلكتروني في المؤسسات وفيما بينها.
3. التعرف على المتطلبات التي تقف حائلاً أمام استخدام التوقيع الإلكتروني مع اختلاف البيئة.
4. الخروج بتوصيات تسهم في ضرورة استخدام التوقيع الإلكتروني في المؤسسات وفي بيئة دراستنا في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية للمحافظة على أمن المعلومات.

ثانياً: اختلفت الدراسة الحالية عن الدراسات السابقة في التالي:

- **بيئة الدراسة:** الدراسة قد تمت في البيئة الداخليـة لمراكـز المعلومـات فـي الجامعـات الفلسطينية حيث أن هيئة تصديق الشهادات تكون جهة داخلية Certificate Authority -CA بينما في الدراسات السابقة فإن هيئة تصديق الشهادات CA تكون جهـة خارجيـة لمراسـلتها إلكترونياً مؤسسات خارجية أي أن الدراسات السابقة طبقـت فـي بيئـة الأعمـال والتجـارة الإلكترونية.

- **مجتمع وعينة الدراسة:** تم اختيار مجتمع الدراسة من جميـع أفـراد مراكـز تكنولوجيـا المعلومات في الجامعات الفلسطينية وليس من أفراد شركات تجارية كما بالدراسات السابقة.

- **متغيرات الدراسة:** ايجاد العلاقة بين متغيرات الدراسة المستقلة(تـوفير سياسـات لحمايـة المعلومات الإلكترونية ،عدم الحاجة للمتطلبات القانونية، تطوير البنية التحتيـة، اهتمـام الإدارة العليا باستخدام تقنية التوقيع الإلكتروني، اعتماد المراسلات الإلكترونيـة داخـل الجامعـات)، والمتغير التابع (متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات فـي الجامعات الفلسطينية في قطاع غزة).

❖ **ما يميز الدراسة الحالية عن البحوث والدراسات السابقة:**

تتميز الدراسة الحالية عن الدراسات السابقة في كونها الأولـى مـن نوعهـا التـي تعـالج متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيـا المعلومـات فـي الجامعـات الفلسطينية، كما أن الدراسة تسعى إلى أهمية المحافظة على سرية المراسلات الإلكترونيـة فـي مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية، وتعمل الدراسة لإنـشاء نمـوذج عملـي لإستخدام التوقيع الإلكتروني وبيان الضرورة إليه.

الفصل الثاني

الإطار النظري

أولاً: التوقيع الإلكتروني

ثانياً: البنية التحتية للمفتاح العام

ثالثاً: الشهادات الرقمية

رابعاً: سلطة منح الشهادات الرقمية

خامساً: سياسات أمن المعلومات

سادساً: حجية التوقيع الإلكتروني

الإطار النظري للتوقيع الإلكتروني

تمهيد

شهد عصر الإتصالات والإنترنت تطوراً كبيراً في مجال المراسلات الإلكترونية والتجارة الإلكترونية فكانت الحاجة إلى ايجاد أدوات أمنية لتواكب هذا التطور لحماية المراسلات الإلكترونية وللحفاظ على سرية وخصوصية المعلومات من الكشف أو التحريف ولإبرام العقود الإلكترونية عبر الإنترنت لتكون بديلاً عن التوقيع التقليدي فنتج التوقيع الإلكتروني (Digital Signature) واعتُرف به بشكل قانوني في العديد من الدول خاصة مع انتشار المعاملات الإلكترونية وقد سنت قوانين وتشريعات خاصة بالتوقيع الإلكتروني لإضفاء الشرعية والصفة القانونية للتوقيع، لتنظم عمل التوقيع الإلكتروني في الكثير من دول العالم، المطالقة (2006).

فالتوقيع الإلكتروني يهدف إلى الحد من مشكلة الأمن والخصوصية على شبكة الإنترنت، فاللجوء إلى التوقيع الإلكتروني يعمل على توفير مستوى متقدم من الأمن والخصوصية للمتعاملين عبر شبكة الإنترنت وشبكة الحاسوب الداخلية للمؤسسات، فالأمن يشغل حيزاً كبيراً من مستخدمي شبكة الإنترنت سواء كانوا مشترين أو مزودين، فالإنترنت مجال مفتوح وغير مسيطر علية من قبل جهة محددة، والإتصال عبر الإنترنت غير آمن، لذلك إنتقال البيانات عبر الإنترنت يزيد من التوقعات في اعتراضها أو تحريفها، فالمعلومات الحساسة يمكن قرائتها من قبل جهات غير مخول لهم الإطلاع عليها، كذلك فالإتفاقيات المبرمة مفترض أن تكون ملزمة لطرفي العقد وأن لا تكون محل خلاف لطرفي العقد فيما بعد. لذلك هناك أربعة احتياجات لا بد من تحقيقهم لإبرام العقود عبر الإنترنت وهي: المصداقية (Authentication)، والخصوصية (Confidentiality or Privacy)، والتكاملية (Integrity)، وعدم الإنكار (non-repudation)، موقع (teletrust.de)، و لأجل ذلك يستخدم التوقيع الإلكتروني لتوفير ثلاثة خدمات أمنية في غاية الأهمية وهي: المصداقية Authentication وتجنب كشف البيانات Data Authentication وعدم تحريف البيانات Data integrity وعدم الإنكار non-Repudiation، دراسة (Hassler, 1999).

1.1 التوقيع الإلكتروني
Digital Signature

1.1.1 ما هو التوقيع الإلكتروني:

التوقيع الإلكتروني هى طريقة لتوقيع الوثائق الإلكترونية، ولمساعدة مستقبل الرسالة من التحقق من مصدر الرسالة ومن هوية المرسل، بالإضافة إلى التحقق من أن محتوى الرسالة لم يجري عليه أي تغيير أثناء ارسالها بعد توقيع المرسل عليها، حيث أن تقنية التوقيع الإلكتروني تمنع المرسل من انكار توقيعه أو جحوده من ارسال الرسالة. فالتوقيع الإلكتروني ليس صورة عن التوقيع التقليدي وانما هو عبارة عن تأشيرة على الوثيقة (Marking a Document) باستخدام المفتاح الخاص(Private key) من قبل المرسل ويتم التحقق منه باستخدام المفتاح العام (Public Key) من قبل مستقبل الرسالة، دراسة Minihan (2001).

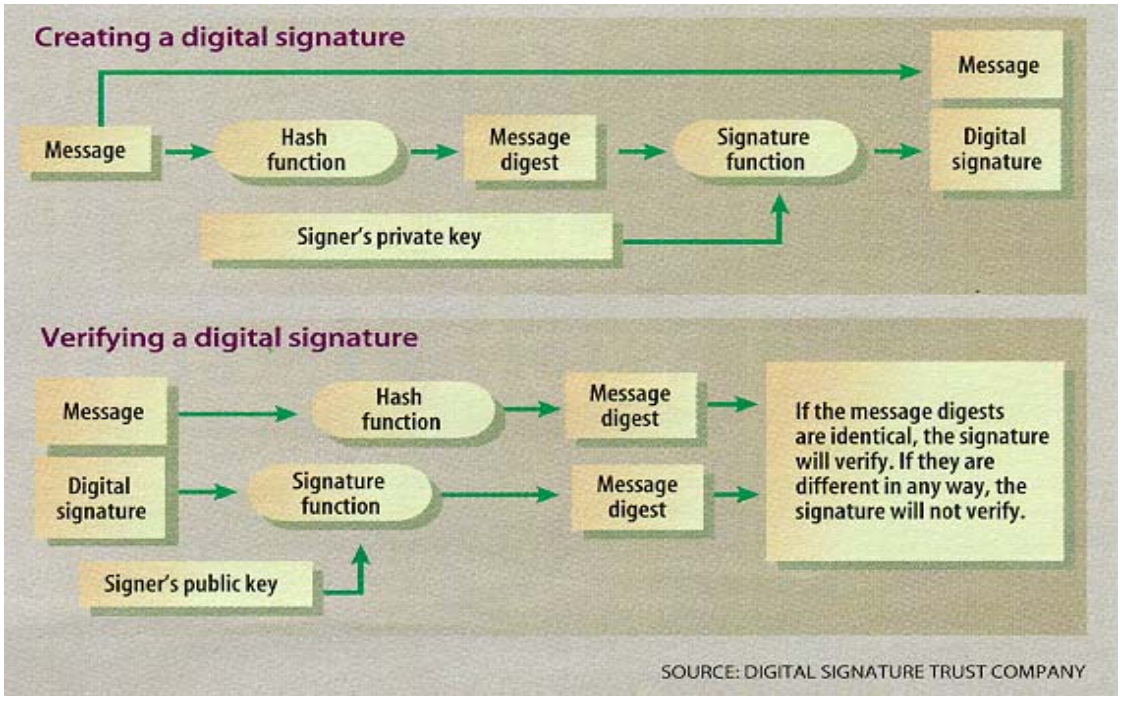
1.1.2 آلية عمل التوقيع الإلكتروني:

في دراسة White (2000) حول آلية عمل التوقيع الإلكتروني فإن الكاتب أكد أن التوقيع الإلكتروني يحقق الموثوقية للمستند المرسل(Authenticity of Massage) و يقوم كذلك بالتحقق من هوية الشخص مرسل الرسالة وحماية هوية المرسل من السرقة.

فعند إرسال مستند موقعاً بالتوقيع الإلكتروني باستخدام برمجيات خاصة بذلك، فإن محتوى المستند (البيانات) تتحول على شكل أرقام (Unique digital representation) وذلك هو نتائج دالة تسمى بالـ (Hash) - دالة رياضية بحتة - وهذة هى المرحلة الأولى. أما في المرحلة الثانية فيمر المستند من خلال دالة التوقيع (Signing Function) ويتم ذلك بواسطة المفتاح الخاصPrivate Key الذي يكون بحوزة المرسل فقط (مرسل الرسالة) أي صاحب التوقيع الإلكتروني الذي يستخدمه من خلال كلمة مرور أو رقم خاص بالمرسل وهنا يقوم المفتاح الخاص بتشفير نتائج دالة الـ hash ويقوم المفتاح العام Public Key بفك تشفيرها وهذة العملية تسمى بصمة التوقيع الإلكتروني (digital fingerprint).

مما سبق يتضح أن الرسالة النهائية التي تكون جاهزة للإرسال تتكون من: المستند، نتائج دالة الـ hash، ودالة التوقيع بواسطة المفتاح الخاص، هذة المكونات مجتمعة تُنشئ التوقيع الإلكتروني، مع العلم ان التوقيع الإلكتروني لا يقوم بتشفير الرسالة ولكن يمكن استخدام نفس تقنية التشفير المستخدمة في التوقيع الإلكتروني في تشفير الرسالة نفسها.

يقوم مستلم الرسالة باستخدم المفتاح العام الذي بحوزته ويكون معروفاً للجميـع والـذي يكـون الخوارزمية الخاصة به في التوقيع الإلكتروني وفي نتائج دالة الـ hash، حيـث أن برمجيـة التوقيع الإلكتروني تختبر فيما إذا كان التوقيع الإلكتروني قد تم إنشاؤه باستخدام المفتاح الخاص والذي يقابله المفتاح العام الذي بحوزة مستقبل الرسالة، الذي يعمل علـى التحقـق مـن هويـة المرسل ومن ان الرسالة مرسله فعلاً من الشخص المقصود. الـشكل (1.1) يوضـح خطـوات إنشاء التوقيع الإلكتروني، دراسة Jones (2000).



الشكل (2.1) خطوات إنشاء التوقيع الإلكتروني، Jones (2000).

1.1.3 خطوات توقيع وتشفير الرسالة الإلكترونية

بينت دراسة شركة CGI (2004) المتخصصة في مجال تكنولوجيا المعلومات وخدمات شركات الأعمال، خطوات التوقيع الإلكتروني عند إرسال رسالة من شخص لأخر على النحـو التالي:

أولاً: توقيع الرسالة (Message Signature): هناك خطوتين يمتلكهما التوقيع الإلكتروني:

a) **Massage Digest Evaluation:** ويهدف للتأكد من ان الرسالة لم يـتم عليهـا أي تحريف أو تغيير أثناء إرسالها وتسمى في هذة الحالة بـ "تكامـل الرسـالة" (Data integrity–) أي سلامة محتوى الرسالة.

b) **Digest Signature:** التوقيع هو عبارة عن تشفير يستخدمه مصدر المفتاح الخاص والذي يحتوي على خوارزميـة الـ Hashing (Hashing Algorithm) ويكـون المفتاح العام تابع للتوقيع أيضاً أي أن المفتاح العام هو الجزء التابع للمفتـاح الخـاص، وبالتالي أي شخص يمتلك المفتاح العام يستطيع أن يفك تشفير الرسـالة ويتحقـق مـن صحة التوقيع الإلكتروني، مما سبق يتضح أن مصدر المفتاح الخـاص يقـوم بتـشفير الرسالة وبذلك تكون الرسالة محمية من أي تغيير عليها أثناء إرسالها.

ثانياً: تشفير الرسالة (Massage Encryption):

a) **إنشاء المفتاحين المتناظرين للتشفير/فك التشفير في نفس الوقت:**
Creation of a One time symmetric encryption/decryption key
تعتبر خوارزمية المفتاحين المتناظرين ذات فعالية كبيرة، لذلك فهي تستخدم بشكل كبير.

b) **تشفير الرسـالة Massage Encryption:** أي يتم تشفير مضمون الرسالة بالكامـل باستخدام المفتاح المتناظرين ويقصد به هنا المفتاح الخاص للتوقيع الإلكتروني.

c) **تشفير المفتاح المتناظر symmetric-Key(SymK) encryption:** يقوم مـستقبل الرسالة فقط بفك تشفير الرسالة باستخدام المفتاح العام الذي يحتوي ضمنياً على المفتاح المتناظر (أي أن المفتاح العام تابع فقط للمفتاح الخاص الذي أستخدم لتوقيع المـستند)، فهو يعتبر ذات حجم صغير من المعلومات مقارنة بالرسالة، وفي حالة إرسال الرسـالة لأكثر من شخص فإن المفتاح المتناظر يختلف من شخص لأخر أي أن المفتـاح العـام المتضمن للمفتاح المتناظر يختلف عن أي مفتاح عام أخر، فلكل توقيع إلكتروني يوجـد مفتاحين، المفتاح العام والمفتاح الخاص بكل توقيع.

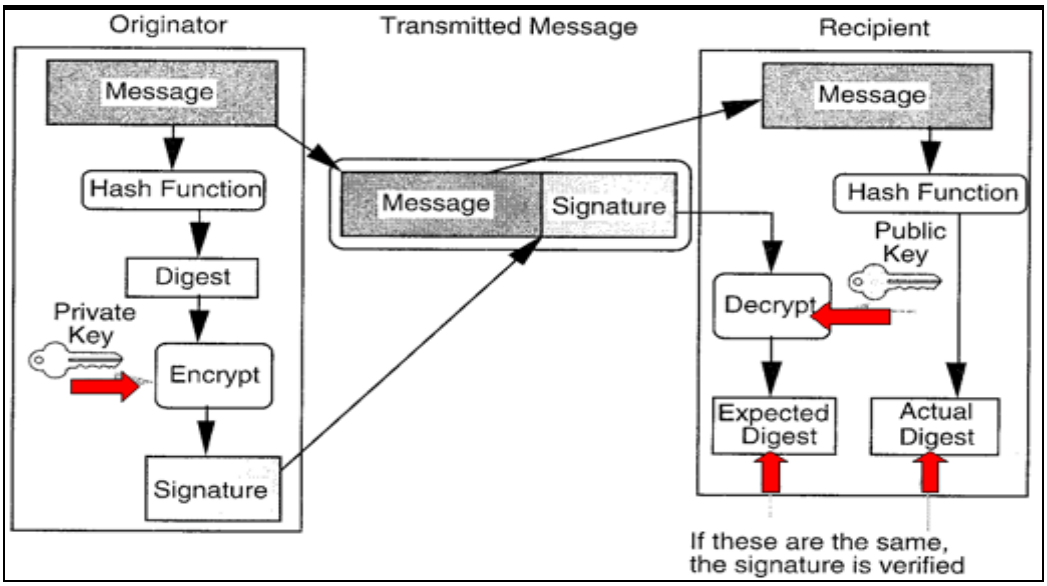
1.1.4 خطوات فك التشفير والتحقق من التوقيع على الرسالة

خطوات فك التشفير والتحقق من التوقيع الإلكتروني هى الطريقة العكسية لفك وتـشفير الرسالة كما وضحتها شركة CGI (2004) على النحو التالي:

اولاً: فك تشفير الرسالة Massage decryption: هناك خطوتين تشفير الرسالة:

a) **فك تشفير المفتاح المتناظر symmetric-key decryption:** المفتاح المتناظر هـو المفتاح الخاص الذي استُخدم في تشفير الرسالة حيث أنه تم فك تشفيره بالمفتاح العـام الموجود لدى مستقبل الرسالة.

b) **فك تشفير الرسالة Massage Decryption:** يستخدم المفتاح المتناظر لفك تـشفير الرسالة (يحتوي على الرسالة والتوقيع معاً).



الشكل (2.2) خطوات توقيع وتشفير الرسالة والتحقق منها، (Arizona State University)

ثانياً: التحقق من التوقيع signature verification: هناك ثلاث خطـوات للتحقـق مـن التوقيع:

a) **Massage digest decryption:** يستخدام المفتاح العام لفك تشفير الـ digest الذي تم إنشاؤه باستخدام المفتاح الخاص لصاحب التوقيع الإلكتروني.

b) **Digest evaluation:** عملية الـ hashing تُنشأ باستخدام المفتاح الخاص وفـي اتجاه واحد من الرسالة، أي أن الرسالة عند المستقبل لا يمكن أن تُشتَق مِن نفـس الـ digest عند إنشائها بالمفتاح الخاص، لذا يجب على المستلم أن يقوم بإعادة تُقيم للـ digest مستخدماً نفس خوارزمية الـ hashing التي استخدمها مصدر الرسالة، لـذلك على مستقبل الرسالة الذي يمتلك المفتاح العام أن يستخدم نفس خوارزمية الـ Hash المستخدمة في تشفير الرسالة.

c) **مقارنة الـ Digests** : في حالة مقارنة نتائج الخطوتين:

- **Massage digest decryption**
- **Digest evaluation**

في حالة تطابقهما فإن التوقيع يكون سليماً وبذلك قد تم التحقق منه وبالتالي يتأكد مستقبل الرسالة من أنه لم يتم أي تغيير على محتوى الرسالة وفي حالة عدم التطابق فإن ذلك يعني أن:

1. الرسالة لم يتم توقيعها من الشخص المقصود.
2. حدوث تغيير على الرسالة أثناء تنقلها.
3. في الحالتين السابقتين فإن الرسالة تعتبر مرفوضة وهذا موضح في الـشكل (1.2) الذي يبين خطوات توقيع وتشفير والتحقق من الرسالة الإلكترونية باسـتخدام التوقيـع الإلكتروني (Arizona State University)

وفي دراسة Borasky (1999) أوضح ان هناك ثلاث خطوات للتوقيع الإلكتروني هى:

أولاً: إنشاء a massage digest: وتعرف أيضاً بدالة الـ hash وتـتم ذلـك باسـتخدام دالـة رياضية (Mathematical Formula) وفـي النتيجـة تتكـون سلـسلة مـن الرمـوز (characters) مرتبطة بالمستند الإلكتروني وبالتالي في حالة أي تغيير تطرأ على المستند سيتكون digest مختلف وبالتالي أي تغيير على المستند سيكتشف في الحال.

ثانياً: استخدام المفتاح الخاص لتشفير الـ digest والذي يتم فك تشفيره لدى مـستقبل الرسـالة باستخدام تقنية التشفير للمفتاح العام(Public key Cryptography)، وهنـا يتـضح أن المفتاح الخاص يستخدم لتشفير الرسلة من قبل المرسل فقط ويستخدم المفتاح العام من قبل المستقبل لفك تشفير الرسالة، ويمكن كذلك استخدام تقنية تشفير المفتاح العام لتشفير مستند وإرساله إلى حامل المفتاح الخاص الذي لا يمكن فك تشفيره إلا باستخدام المفتاح الخـاص فقط (في حال التشفير باستخدام المفتاح الخاص، يستخدم المفتـاح العـام الموجـود لـدى المستقبل لفك التشفير، بينما استخدام نفس المفتاح العام لتشفير المستند، فإنه لا يمكن فـك تشفيره إلا باستخدام المفتاح الخاص التابع له هذا المفتاح العام).

ثالثاً: التحقق من هوية الموقع بواسطة " سلطة منح الشهاداتCertification Authority-CA" والتي عادةُ ما تقوم باصدار زوج المفاتيح الخاصة بالتوقيع الإلكترونـي (المفتـاح العـام والمفتاح الخاص)، وهي سلطة يتم اللجوء إليها للتحقـق مـن هويـة صـاحب التوقيـع الإلكتروني ومن أن المفتاح العام ساري المفعول أم لا.

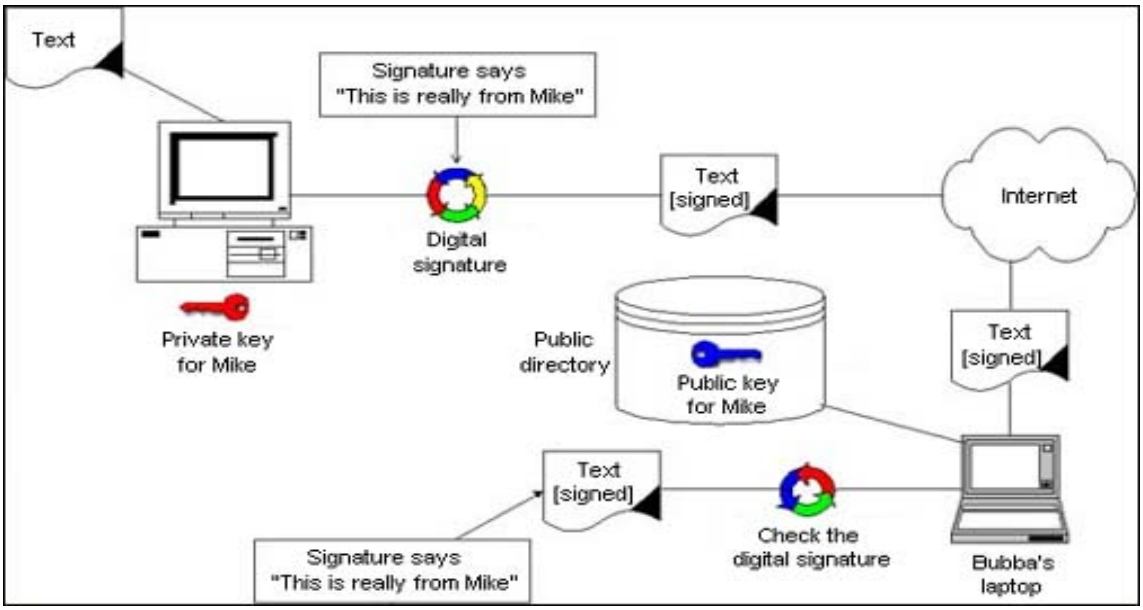
ومن هنا يرى الباحث ان التوقيع الإلكتروني يمر بعدة مراحل للتحقق من سلامة المستند ومـن هوية المرسل وهي:

1. **توقيع وتشفير الرسالة** : وهي تُعد الخطوة الأولى في هـذة المرحلـة لتنفيـذ العمليـة الرياضية (دالة الـ Hash) بالمستند وتكوين ما يسمى بالـ (Massage digest) ومن ثم تشفير الـ Massage digest باستخدام المفتاح الخاص ويكون ناتج ذلـك، التوقيـع الإلكتروني الذي يتم إرسالة ضمن المستند المنوي إرساله.

2. **فك تشفير التوقيع الإلكتروني لدى مستقبل الرسالة**: ويتم ذلك بطرقـة عكـسية عـن الخطوة السابقة رقم (1) "توقيع وتشفير الرسالة" لدى المرسل وذلك بفك تشفير التوقيـع الإلكتروني مرة ثانية إلى الـ Massage digest باستخدام المفتاح العام حيـث فـي النتيجة تتكون دالة الـ Hash مرة أخرى ومن ثم مقارنة الـ Digest Massage التي تم فك تشفيرها باستخدام المفتاح العام مع الـ Digest Massage التي تـم تـشفيرها باستخدام المفتاح الخاص.

3. **في حال تطابق Digest Massage** في كما في المرحلة الثانية السابقة فهذا يعنـي ان الرسالة مرسلة فعلاً من الشخص المقصود وأنه لم يتم عليها أي تحريف أثناء إرسالها.

الخطوات السابقة يتم تنفيذها إلكترونياً من أي جهاز كمبيوتر باستخدام برمجيات خاصة بالتوقيع الإلكتروني، وتتم ذلك بشكل تلقائي دون أن يقوم المستخدم (المرسل أو المـستقبل) بأي مجهود أو أي خطوات يدوية أخرى وقد وضحت شركة IBM مراحـل التحقـق مـن سلامة المستند ومن هوية المرسِل كما في الشكل (2.3)



الشكل (2.3) مراحل التحقق من سلامة المستند ومن هوية المرسل، موقع (IBM.com)

1.1.5 أفضلية التوقيع الإلكتروني مقارنة بالتوقيع التقليدي

بينت جامعة (North Carolina) أن هناك عدة أسباب يتميز بها التوقيع الإلكتروني عن التوقيع التقليدي وهي:

1. **التكاملية(سلامة المحتوى) Integrity**: أي أن البيانات لم يجري عليها أي تغيير أثناء تنقلها، وقد وضح Radcliff (2000) أن مستقبل الرسالة يستطيع عند تلقي الرسالة أن يعرف إن كان هناك تلاعب بالبيانات أوحدوث أي تغيير عليها وهذا يتوافق الرأي مع Horton (2003) الذي بين أنه في حالة ارسال المستند الموقّع باستخدام التوقيع الإلكتروني، وحدوث أي تغيير أو تعديل على المستند أثناء إرساله فإنه بذلك يبطل التوقيع الإلكتروني، وهذا يعني أنه لا يوجد طريقة فعالة لتغيير محتوى الرسالة أو التوقيع الذي عليها أو إنشاء رسالة جديدة بنفس التوقيع الإلكتروني للرسالة السابقة، فإن حصل ذلك فإنه يعتبر تزوير وهذا يعني أن التوقيع الإلكتروني معطلاً .
مما سبق يتضح ان التكاملة تعني انه لم يحصل أي تغيير او تعديل على الرسالة منذ توقيع المرسل عليها واستلامها من قبل المستقبل.

2. **الخصوصية Privacy**: وهي احد مزايا التوقيع الإلكتروني التي تهدف إلى التاكد من ان الشخص المقصود هو فقط من اطلع على المستند المرسل، وبين Horton (2003) أن الخصوصية تعني أن البيانات متوفرة فقط للأشخاص المسموح لهم بالإطلاع عليها، بينما وضح موقع (teletrust.de) ذلك بطرح السؤال التالي/ "كيف أحمي البيانات الخاصة بي من أشخاص غير مخول لهم الإطلاع عليها أو اعتراضها ؟"، بينما الخصوصية في رأي المومني (2003) تعنى أن الرسالة الإلكترونية الموقعة بواسطة التوقيع الإلكتروني لم يطلع عليها أي شخص غير مخول بالإطلاع عليها.
فالخصوصية تعني عدم إطلاع الأخرين غير مخول لهم بالإطلاع على مضمون مستند معين موقعاً بالتوقيع الإلكتروني سوى الشخص المرسل له المخول بالإطلاع عليه.

3. **عدم الإنكار Non-repudiation**: عدم قدرة مستقبل او مرسل الرسالة من إنكارها، وبينت دراسة Radcliff (2000) ذلك حيث آن المفتاح العام يثبت استلام الرسالة من قبل المستقبل وذلك بإرسال رد (إيصال استلام -returns a proof of receipt) إلى المرسل.
فعدم الإنكار- تعني حماية المستند أو العقد الإلكتروني من الإنكار من أحد الطرفين(المرسل أوالمستقبل).

4. **الموثوقية او الإثبات Authentication** : أي التأكد من هوية الشخص المرسِل حيث أن الإثبات يجب أن يجيب على السؤال: من أرسل هذة الرسالة ؟ بينما وضح موقع (teletrust.de) عن ذلك بالسؤال التالى: كيف أعرف من على الطرف الأخر؟ بينما بين موقع (wikipedia.org) أن الإثبات يعني " التحقق من مصدر الرسالة فهي ضمان أن الرسالة قد صدرت من مرسِلها الحقيقي".
الإثبات هو احد المزايا التي يتمتع بها التوقيع الإلكتروني والتي يعني التحقق من هوية الشخص المرسل.

5. **تاريخ توقيع الرسالة Date-Time stamping** : مرسل الرسالة لا يستطيع تغيير تاريخ توقيع وارسال الرسالة وكذلك مستقبل الرسالة حيث ان ذلك له اهمية كبيرة في مجال التجارة الإلكترونية والعقود القانونية.
تاريخ توقيع الرسالة تعني عدم قدرة مرسل الرسالة او مستقبلها من إجراء أي تعديل على تاريخ إرسال أو استلام المستند فهو ملزم للطرفين خاصة في حال إبرام العقود التجارية عبر الإنترنت.

6. **سرعة ودقة انجاز المعاملات Speed & Accuracy**: التوقيع الإلكتروني يزيد من سرعة ودقة المعاملات الإلكترونية ويقلل من تأخر إرسال واستلام العقود والمستندات التجارية حول العالم.

مما سبق يتضح ان التوقيع الإلكتروني يتميز عن التوقيع التقليدي من حيث الخصوصية والإثبات وسلامة المحتوى وعدم الإنكار وهذا موضح بالجدول رقم (2.1) من خلال المقارنة بين التوقيعين الإلكتروني والتقليدي.

جدول رقم (2.1) مقارنة بين التوقيع الإلكتروني والتوقيع التقليدي

#	وجة المقارنة	التوقيع التقليدي	التوقيع الإلكتروني
1	Privacy	• فن (رسم يقوم به الشخص)	• علم(برمجيات)
2	Authentication	• يمكن تزويره أو تقليده • التحقق من التوقيع يحتاج إلى خبراء وحكم قضائي	• لا يمكن تزويره أو تقليده • يتم التحقق من التوقيع تلقائياً(في الحال)
3	Data Integrity	• يمكن الإطلاع علي البيانات من قبل أشخاص أخرين.	• لا يمكن الإطلاع علي البيانات من قبل أشخاص أخرين.
4	Non-Repudiation	• إمكانية تزوير الوثيقة او إقتطاع جزء منها. • إمكانية إجراء تعديل على الوثيقة.	• لا يمكن تزوير الوثيقة او إقتطاع جزء منها. • لا يمكن إجراء أي تعديل على الوثيقة
5	Date-Time stamping	• صاحب التوقيع يستطيع أن يشكك في تاريخ المستند	• صاحب التوقيع لا يستطيع أن يشكك في تاريخ المستند.
6	Speed & Accuracy	• يأخذ وقتاً في الإرسال والإستلام	• سرعة الإرسال و الإستلام

بالإضافة إلى المقارنة الموضحة بين التوقيعين في الجدول رقم (2.1) وضح موقع (entrust.com) مزايا التوقيع الإلكتروني مقارنة بالتوقيع التقليدي بطريقة أخرى كما في الجدول (2.2).

1.1.6 تعريف التوقيع الإلكتروني:

1. التوقيع الإلكتروني "عبارة عن أرقام خاصة (Codes) مشفرة مرتبطة (attached) بالرسالة الإلكترونية، حيث أنها تتيح لمستقبل الرسالة التحقق من الشخص مرسل الرسالة ومن أنه هو فعلاً الشخص الموقع على الرسالة، دراسة Radcliff (2000).

جدول رقم (2.2) مزايا التوقيع الإلكتروني عن التوقيع التقليدي، موقع (Entrust.com)

#	Property	Paper Signatures	Digital Signatures
1	Can be applied to electronic documents and transactions	No	Yes
2	Signature verification can be automated	No	Yes
3	Signature automatically detects alterations to the document	No	Yes
4	Can be used to signify a commitment to a contract or document	Yes	Yes
5	Can be augmented by use of a witness to the signature process	Yes	Yes
6	Recognized by legislation	Yes	Yes

2. التوقيع الإلكتروني "هو مصطلح يستخدم لتوقيع المستند الإلكتروني بطريقة تكون مرادفـة تماماً كما في التوقيع على الورق لكن التوقيع الإلكتروني يستخدم تقنية تشفير المفتاح العـام للتحقق من شخصية المرسِل، موقع (entrust.com).

3. عرف موقع (teletrust.de) التوقيع الإلكتروني بأنه " توقيع أُنشئ بواسطة المفتاح الخاص وأُلحق بالبيانات الإلكترونية ويكون مطابق للختم تماماً ".

4. التوقيع الإلكتروني هو نوع من التـشفير اللامتنـاظر(Asymmetric Cryptography) يستخدم ليفلد خصائص امن التوقيع في شكل رقمي بدلاً مـن الـشكل المكتـوب written Form، موقع (Wikipedia.org.).

5. بينما بينت دراسة Wilson (1999) أن التوقيع الإلكتروني "هو حجم صغير من البيانـات تقوم بالتعرف على مصدر المستند "

6. التوقيع الإلكتروني يحدد هوية المرسل ويتعرف على صاحب الوثيقة وهو عبارة عن خليط مشفر ملحق بالوثيقة ويظهر على شكل صف من الرموز (string of characters) في ذيل الرسالة، دراسة Edward (2004) .

فالتوقيع الإلكتروني: "هو تقنية تستخدم للحفاظ على سرية البيانات وللتحقق من هوية المرسـل باستخدام المفتاح الخاص والمفتاح العام".

يعتقد الكثير ان مفهوم مصطلح "التوقيع الإلكتروني" Electronic Signature" هو نفس مفهوم مصطلح "التوقيع الرقمي" Digital Signature، حيث ان المصطلحين مختلفين من حيث التقنية، ففي حين أن مصطلح Electronic Signature يعني كل أسلوب أو وسـيلة لوضـع الموقع توقيعه لتوثيق المستند بصورة إلكترونية وما يترتب على ذلك من إلتزام قانوني بمضمون المستند، المومني (2002) بينما Digital Signature هو أحد وسـائل التوقيـع الإلكترونـي electronic Signature وهو يتكـون مـن ثـلاث خطـوات هـى: خوارزميـة رياضـية (Mathematical Algorithm) ، التشفير (Encryption)، و الـشهادة الرقميـة (Digital Certificate)، دراسة Borasky (1999) ويعتبر أحد الطرق المضمونة للتحقق مـن هويـة المرسل وبناء الثقة في مجال التجارة الإلكترونية ومراكز البيع، دراسة Radcliff (2000).

فمصطلح الـ Digital Signature بشكل عام هو المصطلح الذي يتم إنشاؤه باستخدام تقنية خاصة لوصـف مـصطلح Electronic Signature ، حيـث أن مـصطلح Digital Signature هو المصطلح الأكثر شيوعاً وتداولاً، دراسة Borasky (1999) وهذا المصطلح هو ما نقصده في دراستنا.
مصطلح التوقيع الإلكتروني العام Electronic Signature يشتمل علـى عـدة أشـكال مـن التواقيع، المومني (2002) منها:

- طباعة إسم المرسل في نهاية الرسالة في حالة البريد الإلكتروني.
- استخدام الرقم الشخصي Personal Identification Number–PIN كمـا الحـال فـي بطاقات الإئتمان.
- إدخال صورة توقيع المرسل الخطي بواسطة الماسح الضوئي إلى جهاز الحاسوب وتوقيـع المرسل للمستند الإلكتروني.
- إنشاء التوقيع الإلكتروني باستخدام الخواص البيومترية (Biometrics Signature) مثـل بصمة الأصبع أو قزحية العين
- التوقيع الرقمي Digital Signature- هو التوقيع الذي يستخدم تقنيـات التـشفير ويمتلـك المفتاح العام والمفتاح الخاص والشهادة الرقمية.

جاءت تسمية التوقيع الرقمي بهذا الإسم بسبب ظهورالتوقيع على شكل سلسلة من الأحرف والخانات الرقمية المشفرة (Stream of Digits) وكذلك نتيجة لاستخدام تقنيات التشفير في إنتاج التوقيع الرقمي، فتقنية Digital Signature تعتبر بديلاً عن التوقيع التقليدي، المومني (2002) وهو المصطلح الذي نقصدة في موضوع هذة الدراسة.

1.2 البنية التحتية للمفتاح العام
Public Key Infrastructure-PKI

البنية التحتية للمفتاح العام -PKI - هي استخدام تقنية التشفير اللامتماثل لإنشاء زوج من المفاتيح أحدهما يستخدم لتشفير الرسالة ويسمى بـ "المفتاح الخاص" التي لا يمكن فك تشفيرها إلا باستخدام المفتاح الأخر الذي يسمى بـ "المفتاح العام "، حيث ان المفتاح الخاص يكون خاصاً بصاحب التوقيع ويحفظ في مكان آمن، بينما المفتاح العام يكون منتشراً لدى العامة، وهذة المفاتيح تستخدم من أجل التوقيع الإلكتروني للبيانات الإلكترونية والإثبات والتشفير، وتقوم الشهادة الرقمية التب تعتبر أحد مكونات PKI بالتحقق من تطابق المفتاح العام مع هوية الشخص الذي صدرت لأجله هذة الشهادة التي تصدر عن جهة مستقلة ذات مصداقية معروفة للجميع، لذلك فإن الـ PKI تعتبر أداه من أدوات الامن الإلكتروني لأنها تتكون من زوج من المفاتيح التي أنشأت من خلال المعادلات الرياضية الخاصة بالتشفير و من الشهادة الرقمية،وهذا ينتج عنة الأمن المطلوب للمراسلات الإلكترونية. والشكل (2.4) يوضح مكونات البنية التحتية للمفتاح العام – PKI، (Michigan Technological University).

إن نجاح العملية التجارية عبر الإنترنت يحتاج إلى توفير ثلاثة عناصر رئيسة لنجاحها، دراسة Kuechler (2002) وهي:

1. **security** : ويقصد به الضمان ان المستند لم يتم عليه أي تغيير بتاتاً أثناء تنقله .
2. **Attribution** : أي أن يكون مصدر المستند معروفاً دون أي شك من هوية المرسل.
3. **Non-repudiation**: ويقصد به أن مرسل المستند لا يستطيع إنكار إرساله للمستند.

فالإطار التقني الذي يمكّن التواقيع الإلكترونية من دعم وتوفير هذه العناصر هي تقنيةُ التشفير المنتشرة والمعروفة قبل ظهور تقنية البنية التحتية للمفتاح العام.

الشكل (2.4) مكونات البنية التحتية للمفتاح العام(Michigan Technological University)

تشفير المفتاح العام يعتبر أفضل طريقة للإتصال الآمن عبر الإنترنت فإنها تدعم نظـام تشفير حيث ان كل مشارك في العقد يوقع بأحد المفاتيح: المفتاح العام ويكون منتشراً لدي الجميع والمفتاح الخاص يكون لدى المرسل فقط، موقع (teletrust.de)، البنية التحتية للمفتـاح العـام PKI تعمل على إدارة الشهادات الرقمية (manage digital Certificates) التي تقوم:

- بتعريف هوية المستخدم وتحتوي على الإسم، الرقم الوظيفي،..إلخ.
- نشر وتعريف المفتاح العام ضروري للتحقق من التوقيع الإلكتروني الخاص بالمستخدم.
- سريان مفعول المـدة الزمنيـة لـصلاحية الـشهادة الرقميـة (Validity Period of the Certificate).

1.2.1 تطبيقات البنية التحتية للمفتاح العام:

هناك عدة استخدامات لتقنية المفتاح العام كما وضحها موقع (teletrust.de) مثل:

1. اتصال الإنترنت الآمن مثل(HTTP) .
2. البريد الإلكتروني الآمن Secure e-Mail.
3. تسديد الصفقات الآمنة Secure payment transactions
4. توقيع المستندات الإلكترونية Signing electronic documents.
5. مساواة التوقيع الإلكتروني بـالتوقيع التقليـدي Electronic signature equivalent to handwritten signature
6. التطبيقات البنكية Banking applications

7. إرسال البيانات بأمان Secure data transfer
8. شبكات الحاسوب الوهمية Virtual private networks - VPN

1.2.2 طرق التحقق من الشخص :

هناك عدة طرق يمكن بواسطتها التحقق من الشخص مثل:

- **كلمة المرور(Password)** : وهي الطريقة الأكثر شيوعاً للتحقق من الشخص وللمحافظة على البيانات الخاصة، ففي حالة عدم تطابق كلمة المرور مع اسم المستخدم فإنـه لا يمكـن الدخول على جهاز الحاسوب او القدرة على استخدام البريد الإلكتروني وبعض البرمجيات.

- **المفتاح الخاص المشفر Private key encryption** : هو عبارة عن كود سري يستطيع تشفير حزمة من المعلومات قبل ارسالها ويكون خاص بمرسل الرسالة فقط حيث أن المفتاح الخاص يكون موجوداً على الكمبيوتر الخاص بالمرسِل لذلك أي شخص يستطيع الولوج إلى المفتاح الخاص فإنه يستطيع تزوير التوقيع الإلكتروني الخاص بالمرسـل، دراسـة Yakal (2000).

1.2.3 طرق حماية المفتاح الخاص

وللمحافظة على المفتاح الخاص من الإستخدام الغير قانوني لغير مالك هذا المفتـاح، فـإن هناك عدة طرق لحماية المفتاح الخاص من الإستخدام الخاطئ، موقع (teletrust.de) منها:

1. **Encrypted storage on magnetic Media** : وهو حفظ المفتاح الخاص بشكل مشفر(Encrypted Form) على وسيلة ممغنطة مثل القـرص الـصلب علـى جهـاز الكمبيوتر الخاص بمالك المفتاح الخاص.
2. **نموذج مستوى الأمن المرتفع بـدون الوصـول للقـراءة High level security modules without read access**: مثل البطاقات الذكية (Smart Cards)، شـرائح المحمول (SIM Cards)، ولتطبيق مستوى الامن المرتفع، فإن المفتاح يجـب أن ينـشأ ويحفظ ويستخدم في مثل هذا النموذج، وبذلك فإن المفتاح الخاص سيكون في مأمن مـن الإستيلاء علية من آخرين غير مخولين بالحصول عليه.

تشفير المفتاح العام يستخدم للتحقق من سلامة الرسالة المرسلة من أي تغيير أثناء ارسالها والتي تم فيها استخدام المفتاح الخاص حيث أن المفتاح العام يكون منتشراً لدى العامـة، موقع (Howstaffworks.com).

1.2.4 خطوات إنشاء وامتلاك واستخدام مفاتيح التوقيع الإلكتروني

الرسالة الموقعة إلكترونياً تشير إلى أنه لم يتم أي تغييرعلى محتوياتها منذ توقيعها وأثناء ارسالها وإلا فإن التوقيع الإلكتروني سوف يظهر خطأ- بمعني أنه معطلاً وهناك خطوات إنشاء وامتلاك واستخدام مفاتيح التوقيع الإلكتروني، موقع (us-cert.gov):

1. انشاء المفتاح (العام والخاص) باستخدام برمجيات خاصة تتميز بالسرية التامة.
2. توفير المعلومات حول المفتاح العام والجهة المالكة لهذا المفتاح للتحقق من هوية المالك وهذا يعمل على زيادة الثقة بين الموقع والأخرين.
3. نشر المفتاح العام للتحقق من هوية المرسل ومن مصداقية الرسالة.
4. توقيع رسائل البريد الإلكتروني الصادرة إلكترونياً.

يختلف التوقيع الإلكتروني عن التوقيع التقليدي من حيث الأسلوب حيث لا يوجد أسلوب معياري للتوقيع التقليدي وبالتالي يختلف كل توقيع تقليدي عن الأخر وهذا يؤدي إلى سهولة تقليده وصعوبة التحقق منه، عكس التوقيع الإلكتروني الذي يعتبر أكثر أمناً من التوقيع التقليدي، لذلك يتوفر في التوقيع الإلكتروني مزايا غير متوفرة في التوقيع التقليدي مثل الشهادات الرقمية.

1.3 الشهادات الرقمية
Digital Certificates(DC)

الشهادة الرقمية هي بمثابة جواز سفر، فهى تعمل على ربط المفتاح العام الخاص بالشخص، أو بالمؤسسة، بهوية المرسل، فهذا الرابط ينفذ من خلال مُصدِر شهادة التوقيع الإلكتروني، كل مشارك بالإتصال يستطيع أن يوضح او يثبت هويته للأخرين بمساعدة الشهادة الرقمية، فهى تصدر عن جهة تسمى سلطة اصدار الشهادات الرقمية (Certificate Authority-CA) والتي تعتبر كجهة ثالثة ذات مصداقية معروفة للجميع (Trusted third Party) للتحقق من تطابق المفتاح العام مع هوية الشخص الذي صدرت لأجله، موقع (Microsoft). فالشهادة الرقمية تعتبر جزء من تقنية البنية التحتية للمفتاح العام PKI وأحد مكوناته، فهى تحتوي على معلومات عن الشخص حامل الشهادة مثل الإسم (هوية حامل الشهادة)، هوية مصدر الشهادة، تاريخ اصدار وانتهاء صلاحية الشهادة، المفتاح العام لحامل الشهادة، المومني (2002)، حيث أنه في حال إنشاء الشهادة الرقمية فإنه يتم توليد زوج من

المفاتيح المشفرة، أحد هذة المفاتيح يكون معروفاً للجميع ويسمى بالمفتـاح العـام Public key والأخر يسمى بالمفتاح الخاص Private Key، ثم تقوم سلطة اصدار الشهادات بإنشاء الشهادة الرقمية وذلك بدمج المعلومات الشخصية الخاصة بالمستخدم مع المعلومات الخاصة بالمؤسـسة المصدرة للشهادة الرقمية مشتملة على المفتاح العام، موقع (Cren.net).

في حالة توقيع المستند باستخدام التوقيع الإلكتروني فإن جميع أجزاء المستند تعتبر موقعة إلكترونياً (لا يمكن اقتطاع جزء من المستند) ولا يمكن إجراء أي تعديل أو تغيير على المـستند وإلا فإن التوقيع الإلكتروني يعتبر معطلاً (Invalid signature) ، كذلك في حـال أن امتلـك شخص ما نسخة من الوثيقة وقام بتغيير إسم مالك الشهادة إلى اسمه لتكون الشهادة ملكاً له، فإنه عند التحقق من التوقيع الإلكتروني الموقع عليها، فإنه سيظهر خطأً وبذلك يكون التوقيع معطلاً. لذلك يعتبر التوقيع الإلكتروني أفضل بكثير من التوقيع التقليدي حيث يثبت أن حامـل الـشهادة الرقمية تعني هو الشخص المقصود مالك هذة الشهادة التي أُصدرت لأجله وليس شخص أخـر، موقع (Cren.net)

التوقيع الإلكتروني عموماً مقبول الأن كتوقيع يتضمن البنية التحتية للمفتاح العام PKI بمعنى هو توقيع يتم إنشاؤه بالوسائل المشفرة التي تضمن استخدام المفتاح العام والمفتاح الخاص الذين يتم إنشاؤهما رياضياً، Department of Information Resources (2002).

1.3.1 وظائف الشهادات الرقمية:

بين موقع (Netscape.com) وظيفتين تقوم بهما الشهادات الرقمية وهى:

1. التحقق من أن حاملى الشهادة الرقمية هم فعلاً من يدعي الحصول على الشهادة الرقمية من حيث كونه شخص أو موقع إنترنت.
2. حماية البيانات من السرقة أو التلاعب أثناء إنتقالها عبر الإنترنت.

بينما أضاف موقع (cren.net) استخدامات أخرى للشهادات الرقمية مثل:

3. التحقق من الأشخاص المتصلين بالـ WebServer أو المتصلين بمصادر شبكة الحاسوب.
4. من أجل تشفير أو توقيع المستندات مثل البريد الإلكتروني.

وأضاف موقع (Netscape.com) أيضاً أن هناك نوعين مهمين من الشهادات الرقمية لا بـد من توافرهما عند بناء موقع إنترنت آمن:

a) **شهادات الخادم Server Certificates :** وتعتبر شهادات مهمة لأى جهة تريد ان تُنشئ موقعاً إلكترونياً تجارياً بحيث أن يكون هذا الموقع آمناً من مخاطر الإختـراق (Threat of Interception) أو التلاعب حيث يسمح لزوار الموقع بتبادل المعلومات الخاصة مثل أرقام بطاقات الإعتماد، ويسمح كذلك بتبادل المعلومات الشخصية مع الزبائن والـوكلاء وبـذلك يشعر زوار الموقع بالآمان من خلال الإتصال بالموقع المقصود ولـيس الإتـصال بموقـع محتال أوموقع ينتحل شخصية موقع آخر.

b) **شهادات الأفراد Personal Certificates :** وهى شهادات تسمح بالتحقق مـن هويـة زوار الموقع حيث أن هناك محتويات مخصصة لا يسمح الوصول إليها للـزوار العـاديين، وهذة الشهادات تُستخدم مثلاً لإرسال بريد إلكتروني آمن إلـى حـساب خـاص (Private Account)، فهذا النوع من الشهادات يصلح تماماً للعمل عبر التجارة الإلكترونية ذات طابع الأعمال (Business to Business - B2B) مثل التحكم على دخول الموردين والـوكلاء على مواقع إنترنت خاصة لتحديث المعلومات لدى الموديين والـوكلاء عـن مـدى تـوفر المنتجات لدى الشركة ومواعيد الشحن وإدارة المخزون.

1.3.2 حالات الشهادة الرقمية:

بينت دراسة Hassler (1999) حالات الشهادة الرقمية حيث تكون الشهادة الرقمية في أحد الحالات التالية:

1. **شهادة سارية المفعول(صالحة) Valid**: وهذا يعني أن الشهادة تكون سـارية المفعـول وتستخدم فعلياً من أجل التحقق والتوقيع.
2. **منتهي الصلاحية Expired**: وتعني ان الشهادة الرقمية منتهية الصلاحية.
3. **المرفوضة Revoked** : وتعني ان الشهادة المذكورة مدرجة ضـمن قائمـة الـشهادات المرفوضة (Certificates Rejected list –CRL).
4. **المؤرشفة Archived** : ويقصد بها أن الشهادة صدرت مسبقاً من قبل سـلطة إصـدار الشهادات ولم تعد تستخدم حالياً وغير متوفرة ضمن الخدمات المقدمة من الشركة مصدرة الشهادة ولكنها موجودة ضمن أرشيف الشهادات التي أصدرتها الشركة.
5. **المتوقفة Suspended**: أي ان الشهادة مرفوضة لمدة محدودة حسب قائمة الـشهادات المرفوضة CRL .

6. **المعدلة Superseded** : أي انه تم إجراء تعديلات على بيانات مالك الشهادة مثل الإسم و العنوان و ... إلخ ومن ثم إصدار شهادة رقمية ثانية لنفس الشخص حسب البيانات المعدلة، أي انه تم عمل Update للبيانات الشخصية التي تتضمنها الشهادة.

1.3.3 الشهادات الرقمية في مؤسسات التعليم العالي

بين موقع (cren.net) أن مركز تكنولوجيا المعلومات في الحرم الجامعي (أو في المؤسسة التعليمية) هو المدخل لإستخدام الشهادات الرقمية من قبل الكليات والطلبة والهيئة التدريسية في الجامعة، وهذا يجب أن يكون مدعوماً من قبل الإدارة العليا للجامعة خاصة أن هذه التقنية تحتل جزء كبيراً من عملية تشغيل وإدارة الحرم الجامعي، فالشهادات الرقمية حالياً تمكن المستخدم من إدارتها بسهولة من خلال متصفح الإنترنت او التطبيقات الخاصة بها، فالشهادات الرقمية والبنية التحتية للمفتاح العام هما تقنيات ذات إمكانيات واسعة وهذا يعني أن بعض مؤسسات التعليم العالي تقوم بنشر تقنية الشهادات الرقمية بشكل واسع للخدمات الجامعية مثل جامعة Columbia **و** Texas-Houston ومؤسسات أخرى تخطط لنشر هذة التقنية مثل جامعة Minnesota **و** Dartmouth ومؤسسات ثالثة تستخدم تقنية البنية التحتية للمفتاح العام PKI Technology الخاصة بها والمنُتجة لديها ومؤسسات أخرى تستخدم مصادر تقنية خارجية كلياً أو جزئياً.

شهادات خادم الإنترنت (Web Server Certificates) هى الشهادات الرقمية الأكثر استخداماً داخل الحرم الجامعي، فهذة الشهادات تسمح بالإتصال المشفر من وإلى الـ WebServer لحماية المعلومات الشخصية الحساسة مثل بطاقة الإعتماد والمعلومات المالية أو الصحية.

1.3.4 استخدامات الشهادات الرقمية:

تستخدم الشهادات الرقمية لأعمال المؤسسات الرسمية أو لعقد الصفقات عبر الإنترنت، أو لتعريف الخوادم وتسمى شهادات الخوادم (Server Certificates)، حيث تتيح فرصة للمستخدم للتأكيد من أنه قد دخل على الموقع المطلوب، كذلك تستخدمها الشركات للحصول على شهادة رقمية خاصة بموقع الشركة لممارسة التجارة الإلكترونية مثل إستقبال أرقام بطاقات الإئتمان الخاصة بالزبائن، وتعتبر التجارة الإلكترونية هى الأكثر استخداماً للشهادات الرقمية، داوود (2004) وبينت دراسة Meckbach (1998) أن للشهادة الرقمية استخدامات متعددة مثل:

1. **توقيع العقود الإلكترونية**: يعتبر التوقيع الإلكتروني أقوى من التوقيع التقليدي حيث لا يمكن تزييفة أو تقليدة عكس التوقيع التقليدي حيث يتم التوقيع الكترونياً على العقد باستخدام المفتاح الخاص والتحقق من التوقيع باستخدام المفتاح العام.

2. **تصديق العقد الإلكتروني:** الشركات دائماً بحاجة إلى تصديق العقد من قبل محامي قـانوني وهذة العملية تستغرق وقتاً عكس التوقيع الإلكتروني الذي يوجد مصداقية متبادلة بين موقعي العقد ولا يحتاج إلى توقيع المحامي.

3. **زيادة الطلب على اصدار الشهادات الرقمية**: ارتفع اجمالي اصـدار الـشهادات الرقميـة الصادرة من شركة (Entrust.com) -شركة إنتاج برمجيات البنية التحتية للمفتـاح العـام PKI- ولإصدار الشهادات الرقمية- لزبائنها من مليون شهادة رقمية إلى 2.5 مليون شـهادة رقمية أي بزيادة 1.5 مليون شهادة رقمية في الفترة ما بين شهري يناير ومارس من العـام 1998، كذلك بالمثل بالنسبة إلى بنك "Scotiabank" حيث أصدر ما يزيـد عـن 40.000 شهادة رقمية للخدمات البنكية عبر الإنترنت حتى منتصف عام 1998.

4. **الإستخدام الآمن للشهادات الرقمية:** فهى تسمح بتوفير تقنيات آمنة دون الحاجة إلى ارسـال كلمات المرور عبر الإنترنت، وهى تستخدم بشكل كبير من قبل المؤسسات المالية والبنكيـة على وجه الخصوص .

1.5 سلطات منح الشهادات الرقمية
Certification Authorities (CA)

سلطة منح الشهادات الرقمية عبارة عن شركة او مؤسسة لإصدار الـشهادات الرقميـة لشركات كانت أو أشخاص، فهي تعتبر جهة مستقلة لها مصداقية تكون إما سلطة مـن خـارج المؤسسة ذات مصداقية مـن الأخـرين أو أن تكـون قـسم مـن داخـل المؤسـسة، موقـع (definethat.com)، فهى سلطة معترف بها لإصدار الشهادات الرقمية للتحقق من الشخـصية ولإصدار شهادة التعريف اللازمة، فهذة السلطات تعمل على التحقق من شخصية مقدم الطلـب

(شخص أو مؤسسة) واصدار وإلغاء الشهادة الرقمية وتوفير معلومات عن الشهادة التي تصدرها لمن يطلب ذلك، داوود (2004).

شهادة التعريف الرقمية تقوم بتوفير معلومات عن صاحب المفتاح الخـاص Private key والمفتاح العام Public key والجهة التابع لها ومدة صلاحية الشهادة والتوقيع الإلكتروني الخاص بسلطة منح الشهادة الموجود على هذة الشهادة مما يثبت صحة الشهادة وأنها صادرة عن هذة السلطة، موقع (Microsoft). فعند إرسال رسالة مشفرة أو استقبال رسالة موقعـة، فـإن الشخص الحامل للمفتاح العام يجب أن يكون قادراً على التحقق من المفتاح العام والجهة التـابع لها هذا المفتاح – أي مالك المفتاح الخاص، موقع (Teletrust.de) ، فسلطة مـنح الـشهادات الرقمية تقوم باصدار وإدارة وإلغاء الشهادات الرقمية، موقع (Cren.net).

المعلومات التي تحتويها الشهادة الرقمية تكون معلومات صحيحة وذات مصداقية بمقدار توافر امن واستقرار سلطة اصدار الشهادات الرقمية، حيث أن معظم سلطات اصدار الـشهادات الرقمية هي عبارة عن شركات تجارية وبسبب السياسات الأمنية المتبعة في هذة الشركات فإنها تحتوي على أعداد هائلة من المتنصلين من مدى صلاحية ودقة الشهادة التي تصدرها وذلـك ان هذة الشركات تحتاج إلى القليل من التحقق من أي شئ أكثر من الشخـصية نفـسها Identity، فشركات الأعمال التجارية القانونية سوف تحتاج إلى اثبات هوية الشركة واستخدامها في الشهادة الرقمية الخاصة بها، دراسة Kuechler (2002).

إذاً مما سبق يتضح أن سلطة إصدار الشهادات الرقمية عبارة عن مؤسسة مـستقلة ذات مصداقية لإصدار الشهادات الرقمية المختلفة الخاصة بالأشخاص أو الخوادم (Servers)، مواقع الإنترنت، والبرمجيات،... إلخ، وذلك من أجل التحقق من هوية مالك المفتاح العام والتاكد مـن صلاحية الشهادة الرقمية بالإضافة إلى تقديم معلومات عن صاحب مفاتيح التوقيـع الإلكترونـي (المفتاح العام والمفتاح الخاص)، فهي مؤسسات تعمل على اصدار الشهادات الرقمية وتوقيـف ورفض هذة الشهادات وتعديل البيانات التي تخص مالك المفتاح العام المنتـشرة عبـر موقـع المؤسسة.

1.5.1 كيفية إصدار الشهادات الرقمية و إلغاءها:

لقد قامت شركة Microsoft ببيان كيفية إصدار الشهادة الرقمية وإلغاءها كالتالي:

1. **إنشاء(توليد) المفتاح Key Generation**: يطلب مقدم الطلب (Applicant) شهادة رقمية من CA وبالتالي يتم توليد زوج من المفاتيح المفتاح العام والمفتاح الخاص.

2. **تطابق سياسة المعلومات** Matching of Policy Information: يقوم مقدم الطلب بتزويد سلطة اصدار الشهادات الرقمية بالبيانات الضرورية الخاصة لإصدار الشهادة للحصول على الشهادة الرقمية مثل الإسم والعنوان ونوع الشهادة و .... إلخ .
3. **إرسال المعلومات والمفتاح العـام** sending of Public keys & Information: يقـوم مقدم الطلب بإرسال البيانات المطلوبة بشكل مشفر لسلطة إصدار الشهادات عبـر الموقـع الخاص بها باستخدام المفتاح العام الخاص بسلطة إصدار الشهادات.
4. **التحقق من المعلومات** Verification of Information: سلطة مـنح الـشهادات تقـوم باعتماد السياسة المناسبة لضمان استلام مقدم الطلب للشهادة الرقمية.
5. **إصدار الشهادة** Certification Creation : تقوم سلطة إصدار الشهادات الرقمية بإصدار مستند رقمي يحتوي على المعلومات المطلوبة حول مقدم الطلب باستخدام المفتاح الخـاص لسلطة منح الشهادات.
6. إرسال/الشهادة بريدياً Sending/Posting of Certificate: سـلطة اصـدار الـشهادات الرقمية يمكنها إرسال الشهادة لمقدم الطلب إلكترونياً أو عبر البريد.
7. تركيـب الـشهادة علـى الجهـاز الخـاص The Certificate is Loaded onto an individual's Computer : أي يتم تركيب (install) الشهادة الرقميـة علـى الجهـاز الخاص لصاحب الشهادة الرقمية.

1.5.2 إلغاء الشهادات الرقمية:

تقوم سلطة منح الشهادات الرقمية باصدار قائمة بالشهادات التي تم إلغاءها CRL مـن قبلها وذلك نتيجة أن حاملي هذة الشهادات أشخاص قاموا بتزويد الـسلطة بمعلومـات غيـر صحيحة او انهم أشخاص ذات شبهات وبالتالي قد استخدموا الشهات الرقمية التي تم إصدارها لهم بطريقة غير صحيحة. إذاً الـ CRL هي عبارة عن طريقة لإلغاء الشهادة الرقميـة بعـد إصدارها، حيث انها تكون معروضة على الموقع الخاص بسلطة إصـدار الـشهادات عبـر الإنترنت.

سلطات إصدار الشهادات CAs ، واستخدام الشهادات الرقميـة DCs تعمـلان علـى تخفيض مشاكل التحقق من انتشار المفتاح العام الخاص بالأشخاص، ومع هذا فالمفتاح العـام الخاص بسلطة إصدار الشهادات الرقمية يعتبر مفتاح ذات مصداقية لدى المستخدمين حيث انه يسمح بالتحقق من الشهادات الرقمية الخاصة بالأخرين.

1.6 سياسات أمن المعلومات
Information Security Polices – ISP

بينت دراسة Kwo-shing Hong (2006) أن سياسات أمن المعلومـات الإلكترونيـة تعتبر كدليل إرشـاد (Guideline of Information Security) لتحـسين مـستوى امـن المعلومات في المؤسسة لحماية بيانات المؤسسة الإلكترونية مـن الاختـراق وذلـك بتحديـد أولويات أمن المعلومات فيها لتنفيذها وإعداد الإجراءات الضرورية لاستخدام هذة الأولويـات في حماية المعلومات الإلكترونية الخاصة بالمؤسسة، فهي تعتبر العمود الفقري في إدارة ودعم تقنيات أمن المعلومات في المؤسسة.، فهي تهدف إلى تقديم الإرشادات لدعم احتياجـات أمـن المعلومات الإلكترونية في المؤسسة وتحديـد المـسؤوليات والـصلاحيات الخاصـة بهـذة المعلومات، فسياسات أمن المعلومات الإلكترونية تعتبر بمثابة معيار يقوم بتحديـد المنتجـات الخاصة بأمن المعلومات التي يجب توفيرها لحماية المعلومات الإلكترونية مـن الإختـراق أو الكشف.

وبناء على دراسة Kostas (2004) فإن المفهوم البسيط لطريقة حماية المعلومات يعتمد على نظام المراقبة المتبعة، حيث أنه في معظم الدول التي تعمل على حماية البيانـات بـشكل عام او حماية قانون الخصوصية، فإن هناك سلطة متخصصة تشرف على تطبيق قانون حماية الخصوصية حيث أن احد الإلتزامات المهمة لحماية الخصوصية هي الحصول علـى اطـار تشريعي، فبقدر أهمية البيانات الشخصية يكون مقدار اتباع المؤسسة لسياسات حمايـة هـذة البيانات التي تكون غالباً متصلة بالعالم الخارجي من خلال صفحة الإنترنت الخاصة بالشركة مثلاً حيث أن مقدار ثقة الزبون بالمؤسسة تعتمد على مقدار سياسات الخصوصية التي تتبعهـا المؤسسة.

1.5.1 سياسات التوقيع الإلكتروني

ويقصد بالسياسات هي الطرق والإجراءات التي تتبعها المؤسسة للحد من الإختراقـات لأمن المعلومات الإلكترونية بشكل عام وبحماية التوقيع الإلكتروني من التزوير بشكل خـاص، فسياسات التوقيع الإلكتروني تعني حماية المفتاح الخاص من الإسـتخدام الخـاطئ لـه وذلـك بالحصول عليه من قبل أشخاص أخرين غير مخولين باستخدامه، فمالك المفتاح الخـاص هـو الشخص الوحيد القادر على استخدامه فقط، موقـع (teletrust.de)، لـذلك وضـعت بعـض

الشركات المصدرة للتوقيع الإلكتروني سياسات خاصة يجب اتباعها للحفاظ علي المفتاح الخاص بحيث أن:

المفتاح الخاص Private Key يجب أن يكون وحيداً Unique بحيث يحمل بصمة شخص واحد فقط (حامله) وأن يدار بشكل أمن Securely Managed في ظل وجود دائـرة حمايـة المعلومات الإلكترونية في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية، ولحمايته يجب أن يحفظ على وسط تخزين مستقل وأمن مثل: جهاز الكمبيوتر المحمـول Laptop، أو PDA، موقع(cren.net), بينما شددت شركة (teletrust.de) أن يتم تخزين المفتاح الخاص على وسط تخزين عالي السرية يمنع إمكانية القراءة مثل البطاقات الذكية Smart Cards ورقاقات جهـاز الهاتف المحمول SIM Cards .

1.5.2 مسؤوليات المستخدم في الجامعات

بينت إدارة مركز تكنولوجيا المعلومات في جامعة Michigan (2002) المـسؤوليات التي تقع على عاتق المستخدم لاستخدام مصادر تكنولوجيا المعلومات في الجامعة وهي:

1. الأخذ بعين الاعتبار خصوصية المـستخدمين (Privacy) وذلـك بعـدم الإطـلاع علـى المعلومات الخاصة بهم أو تغيير كلمات المرور الخاصة بهم.

2. الأخذ بعين الاعتبار الحماية القانونية لحقوق الطبع وقانونية البرمجيـات (Licensing of programs) بحيث لا يتم نسخ هذة البرمجيات واستخدامها للتهرب من دفع الثمن الحقيقـي لها.

3. الأخذ بعين الاعتبار استخدام الموارد الإلكترونية الخاصة بالجامعة للأغـراض والنـشاطات التي تتعلق بعمل الجامعة فقط والتي توفرها الجامعة لمستخدميها بشكل خاص مثل حـسابات المستخدمين Users Accounts (عدم اعطاء اسم المـستخدم وكلمـة المـرور الخاصـة بالمستخدم المقصود لأي شخص أخر أو انجاز أي معاملات إلكترونية أو مالية تحـت اسـم شخص غير مخول بذلك).

4. الأخذ بعين الاعتبـار اسـتخدام أنظمـة التبـادل الإلكترونـي (electronic exchange systems) مثل البريد الإلكتروني بحيث يتم استخدام هـذة الأنظمـة لمـصلحة المؤسـسة والنشاطات التي تتعلق بعمل المؤسسة وليس لأغراض تجارية أو دعائية أو لأغراض تخـل باللوائح والقوانين المتبعة في الجامعة.

5. الأخذ بعين الاعتبار تكامل الأنظمة الإلكترونية (Integrity of the systems) بحيث أن هذة الأنظمة يتم تصميمها وتطويرها بواسطة القسم المشرف على هذة الأنظمة وبذلك لا يستطيع المستخدم أن يخترق هذة الأنظمة أو يقوم باجراء أي تعديل عليها باستثناء الجهة المشرفة عليها.

إن السياسات المدرجة أعلاه تبين أن على جميع موظفي وطلبة الجامعة الإلتزام بجميع سياسات ولوائح الجامعة العامة المتبعة والتي تضمن استخدام مصادر المعلومات الإلكترونية وأجهزة وشبكة الحاسوب والبرامج الخاصة بها والإتصالات بالشكل القانوني والأخلاقي .

وقد اتفقت بعض السياسات التي تتبعها جامعة Michigan (2002) مع السياسات المتبعة في جامعة New York At Stony Brook (2001) على النحو التالي:

1. **الخصوصية (Privacy)**: أي أن المستخدم لا يحق له أن يطلع أو ينسخ أو يحرف أي بيانات إلكترونية خاصة بمستخدم أخر.

2. **حقوق الطبع (Copyright)** : وتعني الحصول على ترخيص مكتوب من الجهة صاحبة الحق للحصول على برامج الحاسوب أو مادة صوتية أو فيديو أو مواد أخري تخدم المسيرة التعليمية.

3. **البرامج (Software)** : أي أن البرامج المستعملة في الجامعة هي برامج يجب أن تكون مرخصة من قبل الجهة المصدرة لهذة البرامج ومحمية حسب القانون لذلك فإن على المستخدمين لهذة البرامج أن يلتزموا بشروط الاستخدام لهذة البرامج حسب الأتفاقية الخاصة بها، وفي حالة الإخلال بالإتفاقية فإنها قد تؤدي إلى معاقبة الموظف الذي أخل بالإتفاقية اوحتى تؤدي إلى إنهاء عمل الموظف من الجامعة.

مركز تكنولوجيا المعلومات في الجامعات هو الجهة التي تتحمل المسؤولية للتأكد من أن البرامج المستخدمة في الجامعة هي برامج مرخصة، لذلك فإن الإتفاقيات أو التراخيص الخاصة باستخدام هذة البرامج يجب مراجعتها باستمرار للتحقق من الإلتزام المستمر بالإتفاقيات الموقعة، كذلك على موظفي الجامعة أن يدركوا ان استخدامهم لهذة البرامج خارج نطاق عملهم يعرضهم للمسائلة القانونية.

4. **التجريح والمضايقة (Harassment, Defamation)** : أي لا يحق لأي مستخدم في أي حال من الأحوال استخدام أجهزة الحاسوب الخاصة بالجامعة لمضايقة أو تجريح أي شخص أخر.

5. **حسابات المستخدمين (User Accounts)** : حسابات الـدخول علـى شـبكة أو أجهـزة أالحاسوب هي حسابات للإستخدام الشخصي فقط وهى حـسابات خاصـة بالنـشاطات ذات العلاقة بعمل الجامعة فقط وكذلك لا يجوز مشاركة الأخرين في استخدامها ويتحمل المستخدم المسؤولية الكاملة في أي استخدام من قبل أي شخص أخر.

6. **السماح بالدخول المحظـور (Permitting unauthorized access)** : أي أن هنـاك صلاحيات تسمح لبعض المسخدمين بعمل اعدادات لبعض البـرامج الخاصـة، أو لأجهـزة الشبكة بحيث يحظر على المستخدمين الأخرين الدخول (الولـوج) إلـى هـذة البـرامج أو الأجهزة لتغيير اعداداتها.

7. **انهاء الوصول لمصادر الجامعة الالكترونية (Termination of access)** : أي أنه عنـد الإنتقال من منصب لأخر داخل الحرم الجامعي أو تـرك الجامعـة أو إنتهـاء الدراسـة أو الإنقطاع لسبب ما فإنه يجب إعادة النظر في الصلاحيات الممنوحة بحيث يتم إنهاء استخدام الحسابات الإلكترونية والامتيازات السابقة في الوضع الجديد.

8. **مراوغة الأمن (Circumventing Security)** : أي أنه يحظر على المستخدمين مـن المحاولة في تدمير أي نظام أمني الكتروني(system's security) معمول به في الجامعـة كما يمنعون من استخدام أي برامج حاسوب لاعتراض أو اكتشاف بيانات أو كلمات المرور.

9. **خرق الأمن (Breaching Security)** : وتعني حظر المحاولات المتعمـدة لخفـض أداء شبكة الحاسوب أو ألأنظمة الإلكترونية المعتمدة في الجامعة والتي قد تؤدي إلى تعطيل عمل الموظفين ومن هذة المحاولات المتعمدة :
   - جلب الفيروسات (Creating or knowingly propagating viruses)
   - الاختراقات (Hacking)
   - فك تشفير كلمة المرور (Password cracking)
   - النظر إلى بيانات غيـر مـصرح الإطـلاع عليهـا (Unauthorized viewing of other's files)

وكما ان هناك مسؤوليات تقع على مسخدم الموارد الإلكترونية في الحرم الجامعي يجب عليه أن يأخذها بعين الاعتبار فإن هناك أيضاً أعمال تندرج ضمن ما يسمى " سوء الاستخدام" ليس لها علاقة بنشاطات الجامعة أو البحث العلمي أو تتعلق بالخدمات التـي تقـدمها الجامعـة للطلبة وللعاملين فيها مثل: استخدام العاب الكمبيوتر، أو الدردشة أو استغلال مـوارد الجامعـة لأغراض تجارية خاصة أو استخدام اجهزة الحاسوب وشبكة الحاسـوب لاغـراض سياسـية، جامعة New York At Stony Brook (2001) والجدول (2.3) يبين المقارنة بين سياسـات تكنولوجيا المعلومات المستخدمه في جامعة نيويورك وجامعة ميتشيغن.

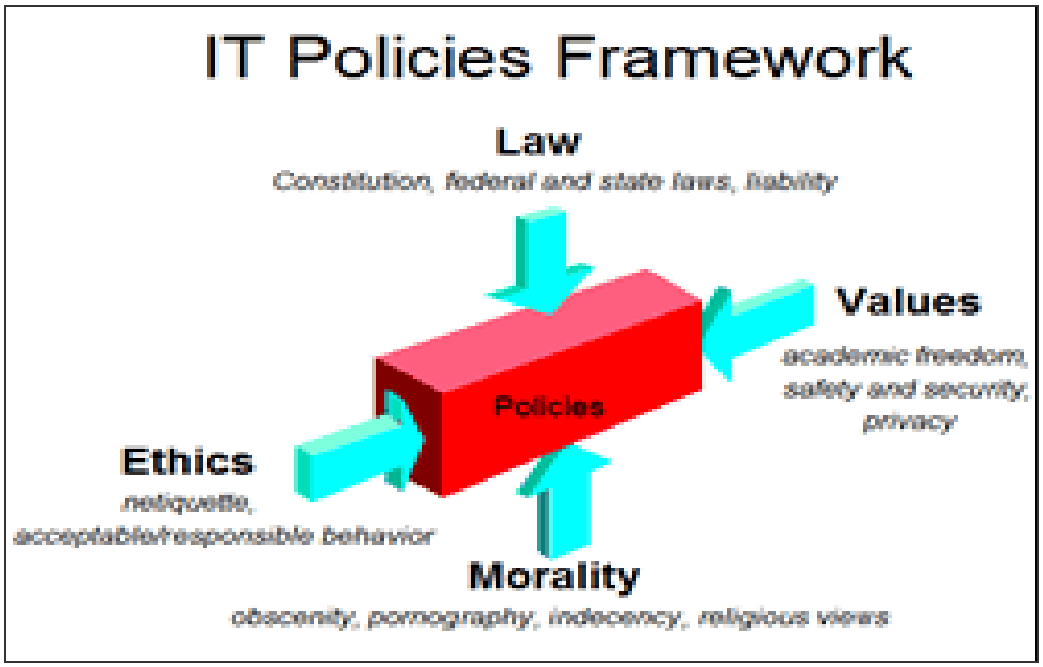
فالسياسات عبارة عن إرشادات وتعليمات يتم إتباعها من قبل المؤسسات بـشكل عـام ومراكز تكنولوجيا المعلومات في الجامعات بشكل خاص وذلك لحماية البيانات الإلكترونية مـن الكشف والإختراق وحتى لا تتعرض هذة الجامعات للمسائلة القانونية أو الأخلاقية أو الأمنية في حال الاستخدام الخاطئ لمصادر تكنولوجيا المعلومات.

جدول (2.3) مقارنة بين السياسات المستخدمة في جامعة نيويورك وجامعة ميتشيغن

#	السياسة المستخدمة	New York	Michigan
1	**Privacy**	√	√
2	**Copyright**	√	
3	**Software(Licensing of programs)**	√	√
4	**electronic exchange systems**		√
5	**Integrity of the systems**		√
6	**Harassment, Defamation**	√	
7	**User Accounts**	√	√
8	**Permitting unauthorized access**	√	
9	**Termination of access**	√	
10	**Circumventing Security**	√	
11	**Breaching Security**	√	

1.5.3 الإطار العام لسياسات تكنولوجيا المعلومات:

إن على الجامعات أن تقوم بتطوير سياسات استخدام مصادر تكنولوجيا المعلومـات لـتلائم أنظمة وقوانين الدولة، فسياسات المؤسسة يتم وضعها حسب إحتياجات المؤسسة الداخلية، لـذلك فهذة الجامعات والكُليات يجِب أن تَتبنّيان إطـاراً شـمولياً يأْخـذُ فـي الحـسبان إعتبـاراتَ: القانون(LAW)، القِيم (Values)، الأخلاق(Ethics)، والمبادىء الأخلاقية(Morality). ويبين أيضاً أن هناك توجه لدى الكليات والجامعات للإلتزام بقوانين الدولة حيث أن هذة القوانين تُملى على الكليات والجامعات ويتم تزويدهم بإرشادات خاصة للعناصر التي يجب أن تؤخـذ بعـين الاعتبار عند وضع السياسات الداخلية للمؤسسة بحيث تتناقض مع القوانين العامة للدولة، لكـن في حالة أن هذة المؤسسات ترغب في حماية المعلومات والبيانات الإلكترونية الداخليـة لـديها مثل: البيانات المالية للمؤسسة فإن هذة المؤسسات يجب أن تحمي وتحافظ على هـذة البيانـات دون الحاجة لقانون أو تشريع لحمايتها، وأن على هذة الكليات والجامعـات أن تتـضمن القـيم الضرورية التي تناسب العمل الأكاديمي بحيث أن يكون توجهها وخبرتها تتناسب والمتطلبـات القانونية لكنهم يجِب أن يكُونوا حريصين على أن لا يتْركوا أو يساوموا قِيم أكاديميةَ مهمةَ، كذلك فإن ادخال القيم الأخلاقية عادةً تكون مفيدة في مجال تكنولوجيا المعلومات لأن القانون لم يتطور أو ينضج بدرجة كافية لتحديد جميع الإنتهاكات المحتملة التي تنشأ نتيجـة تطـور تكنولوجيـا المعلومات، فالسياسات التي تستند على المبادئ الأخلاقية تكـون ذات مرونـة كبيـرة وتمنـع التدخلات التربوية التي أحياناً تعترضها القوانين والتشريعات، فالسياسات المبنية على المبـادئ الأخلاقية تساعد الطلبة والموظفين على حدٍ سواء ليكونوا مواطنين بمستوى أخلاقي أفضل، فهذة المؤسسات تعمل وفق الإلتزامات القانونية والأخلاقية لذلك نجدها تمنع المضايقات الجنـسية أو التربية المعادية لكنها تسمح بحرية الرأي وحرية الكلام وتشجع على الحرية التعليمية، دراسـة Rodney (2004).



شكل رقم (1.4) الإطار العام لسياسات تكنولوجيا المعلومات، Rodney (2004)

إن السياسات الخاصة باستخدام تكنولوجيا المعلومات التي تُوضع من قبل الجامعة لا بد وأن تتناسب مع المتطلبات القانونية العامة للدولة أي وفق القانون بحيث أن على هذة المؤسسات أن تحافظ على القيم والمبادئ الأكاديمية التي تتمتع بها هذة المؤسسات بحيث أن هذة السياسات يجب أن تستند إلى المبادئ الأخلاقية وحرية التعليم وتعمل على منع التـصرفات التـي تخـل بالنظام والأمن العام للمؤسسة.

1.6 حجية التوقيع الإلكتروني
The electronic signature legalism

يعمل التوقيع الإلكتروني على توفير الأمن والخصوصية للمتعاملين عبر شبكة الإنترنت وذلك بالحفاظ على السرية – سرية المعلومات- وذلك بعدم قدرة أي شخص أخر بالإطلاع على المعلومات أو تحريفها، وهناك توجه لدى كافة المؤسسات العامة والخاصة والحكومية لأستخدامه وادخاله في أنظمة العمل لديها مما يعني الإستغناء عـن التوقيـع التقليـدي واحـلال التوقيـع الإلكتروني الذي يعمل على تحديد هوية المرسل والتأكد من المصداقية، ومع ظهور الإنترنـت ونمو التجارة الإلكترونية أدى إلى انتشار المعاملات الإلكترونية مما دعى المؤسسات التشريعية لإصدار تشريع خاص بالتوقيع الإلكتروني لإضفاء الشرعية والصفة القانونية عليه ليكون بـديلاً عن التوقيع التقليدي في التعاملات (الإلكترونية) المالية والتجارية، فالتوقيع الإلكتروني يـستخدم

للتعبير عن إرادة صاحبة الذي يحدد شخصيته فهو عبارة عن مجموعة من البيانات أو الرمـوز يتم ادراجها بشكل الكتروني ويكون مرتبطاً أو مضافاً للرسالة الإلكترونية، وهناك شروط يجب توافرها لصحة التوقيع الإلكتروني، المطالقة (2006):

1.6.1 الشروط القانونية لصحة التوقيع الإلكتروني

يعتبر التوقيع الإلكتروني شكلاً جديداً من أشكال التوقيع فهو توقيع مشابة للتوقيع التقليدي من حيث القيمة القانونية، لذلك لا بد من شروط يجب توافرها لتنظيم قانون التوقيع الإلكترونـي وهي:

1. **وجوب توثيق التوقيع**: أي أنه يجب توثيق التوقيع الإلكتروني لدى جهة معتمدة تُحـدد مـن قبل الحكومة للتحقق من صحة التوقيع.

2. **أن يكون التوقيع مميزاً خاص بالموقع :** أي أن يكون التوقيع الإلكتروني خاص بحامل هذا التوقيع ولا يمكن توافر عدة نسخ للتوقيع الإلكتروني أو اصدار نفس التوقيـع لأكثـر مـن شخص، مما يؤدي إلى إلغاء ميزات التوقيع الإلكتروني التي يمتاز بهـا، وبـين نـصيرات (2005) أن مستقبل الرسالة الموقعة بالتوقيع الإلكتروني يستطيع أن يتحقق من التوقيع عبر سلطة اصدار الشهادات الرقمية CA التي تؤكد صحة التوقيع وذلك يعني أن لكـل شـخص توقيع إلكتروني خاص به مميز عن غيره.

3. **أن يكون التوقيع دليلاً للتعريف بحامل التوقيع:** إن التعريف والتحقق من هويـة الـشخص تعتبر الوظيفة الأساسية للتوقيع الإلكتروني، فتحديد هوية صاحب التوقيع ضروري جـداً لا سيما في المعاملات المالية والتجارية وذلك للتأكد من صحة البيانات المرسـلة مـن قبلـه، فالتوقيع الإلكتروني يعتبر أكثر قدرة على التحقق من هوية حامل التوقيع وأهليته وهذا يمنح الزبائن المتعاملين عبر الإنترنت الثقة والأمان أثناء الشراء أو البيع عبر الإنترنت.

4. **أن يكون التوقيع مرتبطاً بالمستند :** أي أن يكون التوقيع الإلكتروني مرتبطاً ارتباطاً وثيقـاً بالمستند المرسل بحيث لا يمكن فصله عن المستند وهذا يدل على مـدى كفـاءة التقنيـات المستخدمة لتوفير الثقة والأمان لآمن المراسلات الإلكترونية وأحد أسـباب نمـو التجـارة الإلكترونية عبر الإنترنت وأضاف نصيرات (2005) أن التوقيع الإلكتروني يعتمـد علـى مفتاحين (المفتاح العام والمفتاح الخاص) بحيث أن لا أحد يستطيع أن يطلع على مـضمون المستند سوى الشخص الذي يملك المفتاح العام وهذا يدل على أن التوقيع الإلكتروني مرتبطاً

ارتباطاً وثيقاً بالمستند الموقع ولا يمكن فصله وبالتالي لا يستطيع أحد أن يعـدل مـضمون المستند المرسل.

1.6.2 وظائف التوقيع الإلكتروني

وقد بين نصيرات (2005) مدى تحقيق التوقيع الإلكتروني لوظائف التوقيع التقليـدي لتحقيـق الغرض الذي من أجله أُنشأ ومن هذة الوظائف:

- **تحديد هوية شخص الموقع**

أي ان التوقيع يجب أن يحقق وظيفة " تحديد هوية الشخص الموقع" مهما كان شـكل التوقيع، وحيث أن التوقيع الإلكتروني قادر على تحديد هوية الشخص الموقع نتيجـة اسـتخدام المفتاح العام والمفتاح الخاص فإن طرفي الرساله (المرسل والمستقبل) قادران على تحديد هوية بعضهما ولتأكيد ذلك يتميز التوقيع الإلكتروني بوجود جهة مستقلة " سلطة تصديق الـشهادات" التي تقوم بالتحقق من هوية الشخص مالك المفتاح الخاص. وهذا يؤكد ان التوقيـع الإلكترونـي يتفوق على التوقيع التقليدي في قدرته على التحقق من هوية صاحب التوقيع في الحال وفي كـل مرة يتم استخدام التوقيع الإلكتروني.

إذاً التوقيع الإلكتروني يتمتع بقدر كافٍ من الثقة ليقوم بدور التوقيع التقليدي تماماً، فهـو قـادر على تحديد هوية الشخص الموقع في الحال عند استلام المستند الموقع.

- **التعبير عن إرادة الموقع بالموافقة على مضمون المستند**

يفترض القانون أن وضع توقيع الشخص على مستندٍ ما فإنه بذلك قد أقر بما ورد في المستند من مضمون وبالتالي وضع التوقيع على المستند يعتبر تعبيراً بالموافقة من قبل الموقـع بما ورد في المستند . لذلك فالتوقيع الإلكتروني يعبر عن إرادة الشخص بصورة أمنة حيـث أن استخدام المفتاح الخاص في توقيع المستند واستخدام المفتاح العام لفك تشفير المفتـاح الخـاص والتأكد من صحة التوقيع عن طريق سلطة تصديق الشهادات، فإن ذلك يعتبر من الوسائل الآمنة في التعبير عن الإرادة، أي أن الشخص يستخدم توقيعه للتعبير عن موافقتـه علـى مـضمون المستند .

وهذا يتوافق مع قانون الأونسترال النموذجي للتجـارة الإلكترونيـة المـادة الـسابعة، موقـع (uncitral.org) بعنوان "التوقيع" والتي تنص على:

"عندما يشترط القانون وجود توقيع من شخص، يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

1. استخدام طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.
2. كانت هذة الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت مـن أجله رسالة البيانات، في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر".

قانون الأونسترال النموذجي يعتمد على إنشاء مكافئ وظيفي، في الوسائط الإلكترونيـة، لمفاهيم ورقية مثل "الكتابة" و "التوقيع".
حيث يشترط عند توقيع شخص ما على مستند فإن التوقيع يجب ان:
1. يدل على هوية الشخص الموقع وموافقته على المعلومات الواردة في المستند.
2. إتفاق أطراف العقد على استخدام الوسيلة المناسبة لتوقيع المستند.

وهذان الشرطان متوفران في تقنية التوقيع الإلكتروني التي تعمل علـى تحديـد هويـة الشخص المرسل باستخدام المفتاح الخاص الذي يكون مقتصراً استخدامه على حامله وهذا يعني موافقته على البيانات الواردة في المستند المرسل بينما يستخدم المفتاح العام والذي يعتبر الجزء المكمل للمفتاح الخاص للتحقق من هوية المرسِل وهذا يعتبر بمثابة اتفاق بين الطـرفين علـى استخدام تقنية التوقيع الإلكتروني في المراسلات الطرفين وبين، داوود (2004) أنه عند التوقيع على الرسائل الورقية فإن ذلك يعني أن الموقع ملتزم بما ورد في الوثيقة تمامـاً ولا يجـوز أن يحدِث أي تغييرعلى المستند بعد التوقيع كما لا يمكن نسخ التوقيع على مـستند أخـر، كـذلك بالنسبة للتوقيع الإلكتروني فإنه يتم التوقيع من قبل المرسل باستخدام المفتاح الخاص Private Key الوحيد الخاص بالمرسل ويكون مرتبطاً بالرسالة ولا يمكن إجراء أي تغيير على الرسالة، كذلك لا يمكن نسخة أو نقله إلى رسالة أخرى وإلا فإنه يعتبـر توقيعـاً معطـلاً Invalid Signature.

إذاً التوقيع الإلكتروني يستخدم بالدرجة الأولي في المجال التجـاري لتوقيـع العقـود الإلكترونية خوفاً من التحريف أو التزوير وبالتالي بحاجة إلى قانون خـاص يـنظم اسـتخدامه ولتنفيذ العقد الذي تم إبرامه بين طرفي العقد، كذلك يمكن استخدامه في داخل المؤسسات بـشكل عام للمحافظة على سرية وخصوصية المعلومات وهذا لا يحتاج إلى اصـدار قـانون خـاص بالتوقيع الإلكتروني للإستخدام الداخلي في المؤسسات، فالمؤسسة لها الحق في استخدام التقنيـة المناسبة للحفاظ على أمن المعلومات في المؤسسة مـن الكـشف أو التحريـف دون الحاجـة

لإستصدار قانون أو تشريع خاص بهذة التقنية أو تلك لحمايـة المعلومـات الإلكترونيـة فـي المؤسسة وهذا يتوافق مع رأي دراسة Rodney (2004).

لقد قام الباحث بإنشاء تطبيق لتقنية التوقيع الإلكتروني كنموذج للتطبيق، حيث أن الباحث قام باختبار البرنامج وقام باستخدامه بشكل فردي كمرحلة أولى، حيث أن هناك إمكانية لتطوير البرنامج بحيث يمكن استخدامه في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية لحماية المراسلات الإلكترونية داخل الحرم الجامعي، حيث أن للبرنامج القدرة على إنشاء المفتاح العام والمفتاح الخاص والشهادات الرقمية وهى المكونات الأساسية لتقنية التوقيع الإلكتروني، ليستخدم بعد تطويره بما يتناسب وطبيعة عمل المؤسسة، وهذا موضحاً في الباب السادس من الدراسة.

الفصل الثالث

مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة

أولاً: ً: إدارة شؤن تكنولوجيا المعلومات في الجامعة الإسلامية

ثانياً: وحدة تكنولوجيا المعلومات – جامعة الأزهر

ثالثاً: مركز الحاسوب - جامعة الأقصى

رابعاً: مركز تكنولوجيا المعلومات والإتصالات – جامعة القدس المفتوحة

مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة
IT Centers at Palestinian Universities in Gaza Strip

مقدمة:

تعتبر مراكز تكنولوجيا المعلومات (Information technology centers) أو" مراكز الحاسوب -Computer Centers "في الجامعات عموماً البوابة التي من خلالها يتم إدخال التكنولوجيا الحديثة إلى الجامعة وتسخيرها في خدمة العملية الأكاديمية والإدارية. فمركز تكنولوجيا المعلومات هو الجهة التي تقوم بعمل الدراسات المتعلقة بتكنولوجيا المعلومات كذلك مساعدة إدارة الجامعة في اتخاذ القرارات المتعلقة بتكنولوجيا المعلومات من خلال توفير الإحصائيات الخاصة بتكنولوجيا المعلومات.

مراكز تكنولوجيا المعلومات هى الجهة التي تقوم بانشاء البـرامج الخاصـة بالعمليـة الأكاديمية مثل برامج القبول والتسجيل و بحوسبة دوائر الجامعة مثل الـدائرة الماليـة وتقـديم الخدمات للطلبة إلكترونياً مثل برامج المكتبات وغيرها، فدور مركز تكنولوجيا المعلومات فـي الجامعة هى توظيف التكنولوجيا الحديثة لخدمة العملية الأكاديمية والإدارية.

تقوم مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية بتقـديم خـدمات تكنولوجيـا المعلومات من خلال إنشاء وتحديث شبكة الحاسوب في الجامعة بشكل مستمر لمواكبة التطـور التقني لتلبية احتياجات العمل في الجامعة، تحديث Update صفحة الويب الخاصـة بالجامعـة' حوسبة دوائر الجامعة من خلال إنشاءالبرامج الخاصة بكل دائـرة، صـيانة وتطـوير أجهـزة الحاسوب، تقديم الدعم الفني لمستخدمي الحاسوب، تدريب الطلبة خريجي الكليات التقنيـة مثـل طلبة كلية الهندسة وتكنولوجيا المعلومات،.... إلخ.

لقد وجد الباحث مسميات عدة لمراكز تكنولوجيا المعلومات في الجامعات الفلسطينية مثل مسمى "إدارة شؤون تكنولوجيا المعلومات" في الجامعة الإسلامية، بينما مسمى "مركز الحاسوب" في كلٍ من جامعة الأقصى و جامعة القدس المفتوحة بينما المـسمى بجامعـة الأزهـر "وحـدة تكنولوجيا المعلومات" وهذا المسمى يقوم بتوفير الخدمات التـي توفرهـا مراكـز تكنولوجيـا

المعلومات في الجامعات الأخرى مثل الصيانة والدعم الفني والبرمجة وإدارة الشبكات لكن هـذا المسمى يكون حسب الهيكلية الإدارية للجامعة التابع لها.

من الملاحظ أن مدى استخدام وتوظيف الجامعة لتكنولوجيا المعلومات ينعكس بالإيجاب على آداء الجامعة وعلى مستوى تقديم الخدمات للطلبة والموظفين وهذا يعكـس مـدى تطـور الجامعة تكنولوجياً حيث يوجد في قطاع غزة خمس جامعات فلسطينية هي:

1. الجامعة الإسلامية.
2. جامعة الأزهر.
3. جامعة الأقصى.
4. جامعة القدس المفتوحة (فرع غزة).
5. جامعة فلسطين.

وقد قام الباحث باستثناء مركز تكنولوجيا المعلومات في جامعة فلسطين مـن الدراسـة لحداثة نشأتها وإلى عدم اعتراف وزارة التربية والتعليم العالي بالجامعة كبقيـة الجامعـات الأخرى ومن خلال الزيارة الميدانية التي قام بها الباحث للجامعة فـإن مركـز تكنولوجيـا المعلومات في الجامعة هو في طور الإنشاء حالياً وفي مرحلة بناء البنيـة التحتيـة لـشبكة الحاسوب في الجامعة، لذا فضل الباحث إستثناء مركز تكنولوجيا المعلومـات فـي جامعـة فلسطين مما قد يؤثر سلباً على نتائج الدراسة.

جميع مراكز تكنولوجيا المعلومات في هذة الجامعات تعمـل علـى توظيـف التكنولوجيـا الحديثة لخدمة العملية الأكاديمية والمستويات الإدارية.

أولاً: إدارة شؤون تكنولوجيا المعلومات - الجامعة الإسلامية.

تمتلك تكنولوجيا المعلومات أهمية كبيرة في الجامعة الإسلامية وذلك من خلال الهيكليـة الإدارية الخاصة بتكنولوجيا المعلومات في الجامعة حيث أنه يوجد منـصب بمـسمى " نائـب الرئيس – رئيس الجامعة- لشؤون تكنولوجيا المعلومات" والذي يقوم بـالتخطيط والإشـراف وتطوير تكنولوجيا المعلومات وتوفير التقارير المتعلقة بتكنولوجيا المعلومات لرئاسة الجامعة مع وجود إثنين من المساعدين لنائب الرئيس لشؤون تكنولوجيا المعلومات هما:

- مساعد نائب الرئيس لشؤون تكنولوجيا المعلومات- مجال الخدمات الإداريةوالفنية.
- مساعد نائب الرئيس لشؤون تكنولوجيا المعلومات – المجال الأكاديمي.

الهدف من إنشاء مركز تكنولوجيا المعلومات وهو تحت مسمى " إدارة تكنولوجيا المعلومـات" هو مساعدة إدارة الجامعة على اتخاذ القرارات المتعلقة بتكنولوجيا المعلومات بالإضـافة إلـى

التخطيط والتنفيذ والإشراف على الأعمال والمشاريع ذات الصلة بتكنولوجيا المعلومات (دليـل تكنولوجيا المعلومات 2005 –الجامعة الإسلامية).

تقوم إدارة تكنولوجيا المعلومات بالجامعة الإسلامية بتنفيذ المهام التالية:

1. وضع إستراتيجية تكنولوجيا المعلومات للجامعة لتوظيف التكنولوجيا في المجال الإداري والأكاديمي.
2. وضع السياسات المتعلقة باستخدام تكنولوجيا المعلومات في الجامعة.
3. توفير الخدمات المتعلقة بتكنولوجيا المعلومات وتطويرها.
4. حوسبة الأنظمة الإدارية والأكاديمية المعمول بها في الجامعة.
5. تقديم كافة الخدمات التقنية وخدمات تكنولوجيا المعلومات للطلبة والموظفين علـى حـدٍ سواء.
6. تقديم الحلول التقنية المناسبة لتطوير العملية الأكاديمية والإدارية.
7. تمثيل الجامعة في المؤتمرات والمعارض المتخصصة بتكنولوجيا المعلومات.

مجالات عمل إدارة شؤون تكنولوجيا المعلومات في الجامعة الإسلامية:

تعمل إدارة شؤون تكنولوجيا المعلومات في الجامعة الإسـلامية فـي عـدة مجـالات المعلومات (دليل تكنولوجيا المعلومات 2005 –الجامعة الإسلامية) وهي:

1. **المجال الأكاديمي:** وذلك من خلال تطوير دائرة التعليم الالكتروني، لتصبح جزءا أساسياً من العملية الأكاديمية في الجامعة ولتدريب الكادر الأكاديمي على استخدام التكنولوجيا الحديثة في العملية التعليمية، وكذلك تطوير الخدمات الأكاديمية مثل المكتبات الالكترونية والإشتراك فـي المؤتمرات والندوات العلمية عبر الدائرة التلفزيونية المغلقـة videoconference وإنـشاء صفحات انترنت خاصة بالطلبة والمدرسين على موقع الجامعة.
2. **المجال الإداري:** وذلك بحوسبة الأنظمة الإدارية والأكاديمية المعتمـدة فـي إدارة العمليـة الإدارية و الأكاديمية مثل برامج: القبول والتسجيل والدائرة المالية وغيرها.

3. **المجال التنموي**: يقوم المجال التنموي لتكنولوجيا المعلومات من خلال:

- عقد اتفاقيات مع شركات عالمية لفتح فروع لها في الجامعة مثل شركة Intel،
- تأهيل خريجي الكليات التقنية وخلق فرص عمل في مجال تكنولوجيا المعلومات من خلال إنشاء حاضنات تكنولوجيا المعلومات.
- توفير مصادر الدعم المادي للمشاريع المتعلقة بتكنولوجيا المعلومات في الجامعة.

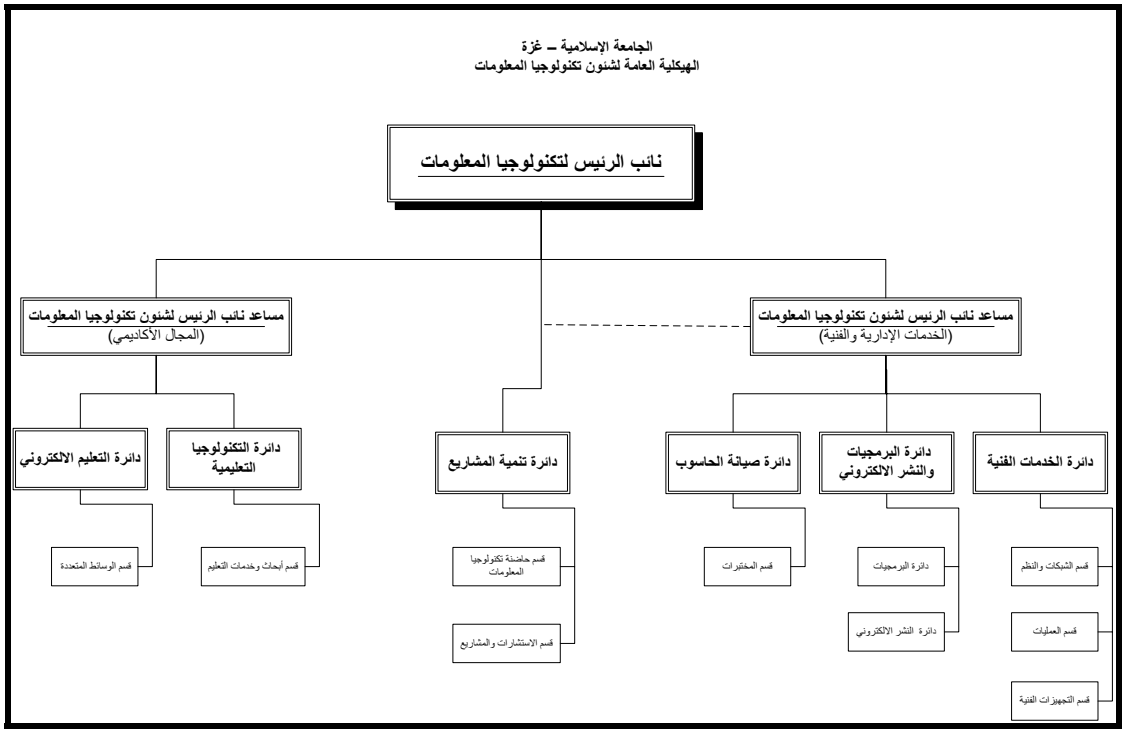
4. **المجال الخدماتي:** تقوم إدارة تكنولوجيا المعلومات بتقديم الخدمات التالية:

- تطوير أجهزة الحاسوب وملحقاتها وإدارة شبكة الحاسوب والخوادم الحاسوبية التابعة لها مع توفير خدمات الصيانة لأجهزة الحاسوب وملحقاتها.
- تقديم الدعم الفني للطلبة والموظفين في مجال تكنولوجيا المعلومات.
- توفير خدمات الانترنت والبريد الالكتروني وخدمات تخزين لبيانات للطلبة والموظفين.
- توفير خدمات النشر الالكتروني مثل تصميم الصفحات الالكترونية الخاصة بالكادر الأكاديمي ونشرها على صفحة الجامعة.

هيكلية إدارة تكنولوجيا المعلومات

يرأس شئون تكنولوجيا المعلومات نائب رئيس الجامعه لشئون تكنولوجيا المعلومات مع وجـود إثنين من المساعدين لنائب الرئيس لشؤون تكنولوجيا المعلومات كما هو موضح في الشكل (1-3) هما:

- مساعد نائب الرئيس لشؤون تكنولوجيا المعلومات- مجال الخدمات الإداريةوالفنية
- مساعد نائب الرئيس لشؤون تكنولوجيا المعلومات – المجال الأكاديمي



الشكل (1-3) هيكلية إدارة تكنولوجيا المعلومات – الجامعة الإسلامية (موقع الجامعة الإسلامية)

فمساعد نائب الرئيس لشؤون تكنولوجيا المعلومات- مجال الخدمات الإداريةوالفنيـة هـو رئيس إدارة تكنولوجيا المعلومات (مركز الحاسوب سابقاً) وهى أحد فرعي شـؤون تكنولوجيـا المعلومات في الجامعة لتقديم الخدمات الإدارية والفنية وتتكون من ثلاث دوائر رئيسية هي:

1. دائرة الخدمات الفنية:

تقوم دائرة الخدمات الفنية بتطوير وإدارة شبكة الحاسـوب وحمايتهـا مـن الإختراقـات ومراقبة آداء شبكة الحاسوب،وكذلك ربط جميع أفرع الجامعة بشبكة الحاسوب، فدائرة الخدمات الفنية هى الجهة التي تعمل على حماية الأنظمة من الإختراقات والحفاظ علـى أمـن وسـرية البيانات وحمايتها، بالإضافة إلى الإشراف على نظم التشغيل وتطويرهـا، والقيـام بعمليـات التخزين الإحتياطي للبيانات Backup واستعادتها Restore، وتقـديم الخـدمات الإلكترونيـة للطلبة والموظفين مثل خدمة البريد الإلكتروني والإنترنت وحفظ بيانات المـستخدمين، وتـوفير الدعم الفني للمستخدمين.

دائرة الخدمات الفنية تقوم بالإشراف على توسعة شبكة الحاسوب من خلال تمديدات الشبكة في المباني الجديدة وتركيب الموزعات الضرورية لذلك أو من خلال تركيب نقاط شبكة جديدة في المباني القائمة، وتعمل على مراقبة الشبكة بشكل مستمر ولاتصرف السريع عند الحاجة لضمان عمل الشبكة على مدار الساعة (Availability)،

تستخدم شبكة الحاسوب في الجامعة تقنية عالية الجودة وذات سرعة عالية تصل إلى1Gbps حيث يتم ربط جميع مباني الجامعة بكوابل الألياف الضوئية Fiber Optics واستخدام الكوابـل النحاسية FTP داخل مباني الجامعة بين الموزعات الفرعية بـسرعة 10/100Mbps، بينمـا يستخدم الإتصال اللاسلكي للربط بين مقر الجامعة في خانيونس مقر كلية مجتمع العلوم المهنية والتطبيقية في جنوب غزة (دليل تكنولوجيا المعلومات 2005 –الجامعة الإسلامية).

تتكون شبكة الحاسوب من 17 خـادم(Server) و224 مـوزع شـبكة(Switch/Hub) وبسرعة تراسل 10/100Mbps، كما تحتوي على أجهـزة لحمايـة شـبكة الحاسـوب مـن الإختراقات مثل الجدار الناري (Firewall) ومضادات للفيروسـات (Antivirus)، وتمتلـك مزودين لخدمة توصيل الإنترنت بسرعة 1.5Mbps، وهناك إحصائيات حول الشبكة (المقابلات الشخصية ودليل مركز تكنولوجيا المعلومات 2005) في المقر الرئيس للجامعة فقط على النحو التالي:

جدول رقم (1-3) إحصائيات حول شبكة الحاسوب والأجهزة المتصلة بها في الجامعة الإسلامية

البند	العدد
نقاط الشبكة	3650
مشتركي خدمة البريد الإلكتروني	1784
مشتركي خدمة الإنترنت داخل الجامعة	900
موزعات الشبكة	224
عدد الأجهزة المركزية Servers	17
أجهزة الحاسوب	2700

تقوم دائرة الخدمات الفنية بتقديم الدعم الفني لمستخدمي الحاسوب في الجامعة، فهى واجهة إدارة تكنولوجيا المعلومات مع مستخدمي الحاسوب، حيث تقوم الدائرة بتقديم الدعم الفني للموظفين من خلال مساعدتهم في الإستخدام الأمثل لأجهزة الحاسوب والعمل على حل المشاكل التي تواجه الموظف في استخدام البرمجيات والقضاء على الفيروسات التي تصيب أجهزة المستخدمين والرد على استفساراتهم عبر التلفون أو عبر البريد الإلكتروني أو بالإتصال عن بعد بجهاز حاسوب المستخدم من خلال برمجيات متخصصة، كذلك العمل على ايجاد البرمجيات المناسبة الجاهزة لساعدة المستخدمين في انجاز أعمالهم، وتقديم خدمات الإشتراك بالإنترنت والإشتراك بشبكة الحاسوب (User Account).

2. دائرة البرمجيات والنشر الإلكتروني.

تقوم دائرة البرمجيات والنشر الإلكتروني بانشاء وتطوير البرامج الداعمة للعملية الأكاديمية ولمساعدة الدوائر الإدارية في انجاز وتقديم خدماتها إلكترونياً،فالدائرة تقوم بالإشراف على قواعد البيانات الخاصة بالبرامج المنتجة في الدائرة.

فالهدف من دائرة البرمجة والنشر الإلكتروني هو تطوير البرمجيات والتطبيقات لمساندة العملية الإدارية والأكاديمية لإنتاج النظام الإلكتروني الشامل في جميع دوائر وكليات الجامعة.

تعتمد دائرة البرمجة والنشر الإلكتروني قاعدة بيانات قوية يتم بناء أنظمة الجامعة عليها، وتعمل الدائرة على حوسبة العديد من الأنظمة وتحويل العديد من الإجراءات الإدارية اليدوية إلى

المحوسبة مثل:-برامج القبول والتسجيل التي تعمل إلى أتمتة أعمال القبول والتـسجيل للطلبـة، وبرامج الشئون الأكاديمية لمتابعة الجداول الدراسية ونظام الامتحانـات وإدخـال العلامـات، وبرامج الشئون الإدارية لمتابعة شئون الموظفين، كالدوام اليومي والإجازات بجميـع أنواعهـا، وبرامج الدائرة المالية وبرامج شئون الطلاب ، وبرامج الدائرة الطبية، وبرامج دائرة اللـوازم والمشتريات، وبرامج المكتبة المركزية، وبرنامج مختبر المواد والتربة، وبرامج التحاليل الطبية. تقوم دائرة البرمجة والنشر الإلكتروني بالإشراف على موقـع الجامعـة وتـصميم الـصفحات الإلكترونية كذلك الإشراف على نظام الـ Portal الأكاديمي، ومساعدة الدوائر والكليات بإنشاء الصفحات الإلكترونية الخاصة بكل دائرة أو كلية، والعمـل علـى تطـوير وسـائل الإعـلان الإلكتروني باستخدام التقنيات الحديثة المتطورة(دليل تكنولوجيا المعلومـات 2005 –الجامعـة الإسلامية).

3. دائرة صيانة الحاسوب.

تهدف دائرة الصيانة إلى توفير الخدمة السريعة لـصيانة أجهـزة الحاسـوب وملحقاتهـا وتحديثها بشكل مستمر ورفع التوصيات للجهات المعنية.

تقوم دائرة صيانة الحاسوب بصيانة أجهزة الحاسوب وملحقاتها من: طابعات، شاشات، UPS ...إلخ، فهى تعمل على تحديث وتطوير أجهزة المستخدمين (موظفين ومختبرات الطلاب)، حيث تقوم بوضع المواصفات المناسبة للأجهزة المطلوبة والقيام بالفحص الفني لهذة الأجهزة، كـذلك تقوم الدائرة بمتابعة الضمانه لهذة الأجهزة مع الشركات الموردة في فترة ما بعد عملية التوريد، وتقوم الدائرة برفع توصياتها لرئاسة الجامعة بخصوص المناقـصات والممارسـات المتعلقـة بأجهزة الحاسوب وملحقاتها(دليل تكنولوجيا المعلومات 2005 –الجامعة الإسلامية).

- **قسم المختبرات:** هو قسم ضمن دائرة الصيانة حيث يقوم بالإشراف العام على مختبرات الحاسوب في الجامعة من حيث الصيانة وتنزيل البرامج الخاصة بالمساقات كذلك يعمل علـى رفع التوصيات المتعلقة بتطوير أجهزة حاسوب المختبرات، ولتحسين مستوى الخدمة المقدمة للطلبة مثل فتح مختبرات خاصة بالإنترنت Open LAB و التسجيل الفصلي للطلبـة خـلال فترة الدوام (موقع الجامعة الإسلامية).

4. دائرة تنمية المشاريع

تتكون دائرة تنمية المشاريع من :

- **قسم حاضنة تكنولوجيا المعلومـات**: ويعمل على انجاز مشاريع مميزة في مجال الحاسوب من خلال الإستفادة من الطلبة الخريجين (خريجي كلية تكنولوجيا المعلومات وكلية الهندسـة)، خاصة المتميزين والذين لديهم أفكار إبداعية لتنفيذ مشاريع مميزة، فالحاضنة تعمل على توفير الخبرة العملية لهؤلاء الطلبة الخريجين لتمكينهم من الحصول على فرص عمل فـي الـسوق المحلي والأجنبي.
- **قسم الإستشارات وتطوير المشاريع**: يعمل على إدارة وتنفيذ مشاريع تتعلـق بتكنولوجيـا المعلومات للمؤسسات التجارية، وكذلك تقديم الإستشارات في مجال تكنولوجيـا المعلومـات للمؤسسات ذات الصلة.

5. دائرة التعليم الإلكتروني

وتهدف إلى استخدام التكنولوجيا في التعليم وتطوير أساليب التعليم التقليدية واستخدام التقنيات الحديثة في التعليم، لذلك تقوم دائرة التعليم الإلكتروني بتدريب المدرسين على استخدام التقنيـات الحديثة لمساعدتهم في طرح مادة المساق بشكل مبسط، فهى كذلك تقوم بتوفير التقنيات اللازمة لتطوير العملية الاكاديمية وعقد ورشات عمل للمدرسين لتطوير أساليب التعليم ورفع مـستوى العملية التعليمية.

من خلال قيام الباحث بالزيارات الميدانية لدوائر وأقـسام إدارة تكنولوجيـا المعلومـات والاطلاع على طبيعة عمل ومهام كل دائرة وقسم، تبين للباحث أن هناك دوائر وأقسام مدرجـة ضمن الهيكلية التنظيمية لإدارة شؤون تكنولوجيا المعلومات بينما فعلياً غير موجودة نتيجة انها قيد الإنشاء أو ان الهيكلية الحالية هى التصور التي ستكون علية إدارة تكنولوجيا المعلومات على المدى البعيد، مثال ذلك حسب الهيكلية التنظيمية المعلنة تتكون دائرة الخدمات الفنية من ثلاثـة أقسام هي: قسم الشبكات والنظم، قسم العمليات وقسم التجهيزات الفنية، لكن هذة الأقسام غيـر موجودة ضمن عمل الدائرة بينما الموظفين الموجودين يقومون بالمهام المطلوبة مـنهم حـسب الوصف الوظيفي كلٌ حسب تخصصه دون وجود مسمى فعلى للقسم أو وجـود رئـيس قـسم مسؤول عن هذا القسم، إنما يعمل الجميع ضمن دائرة الخدمات الفنية فقط.

دائرة تنمية المشاريع المدرجة ضمن الهيكلية التنظيمية فهى لم يتم تكوينها بعد إنما هناك قسم حاضنة تكنولوجيا المعلومات فقط في طور الإنشاء. وكذلك الحال بالنسبة لـدائرة التكنولوجيـا التعليمية لم يتم إنشاءها بعد على أرض الواقع، لكن دائرة التعلـيم الإلكترونـي فهـى الـدائرة الموجودة الوحيدة ضمن المجال الاكاديمي والذي يرأسها مساعد نائب الرئيس لشؤون تكنولوجيا

المعلومات –المجال الأكاديمي دون وجود لقسم الوسائط المتعـددة المـدرج حـسب الهيكليـة التنظيمية لإدارة تكنولوجيا المعلومات.

من خلال ما سبق فإن شؤون تكنولوجيا المعلومات بحاجة إلى اهتمام أكبر من قبـل القـائمين عليها لتنفيذ الهيكلية التنظيمية الموضوعة لها لستطيع ان تقوم بالمهام الملقاه عليها علـى أكمـل وجة وعمل تقييم مستمر لإنجازات شؤون تكنولوجيا المعلومات لتتمكن إدارة الجامعة من تحديد نقاط الضعف التي تعيق العمل بالهيكلية حسب التصور الموضوع لها (دليل تكنولوجيا المعلومات 2005 –الجامعة الإسلامية).

ثانياً: وحدة تكنولوجيا المعلومات - جامعة الأزهر

تأسس مركز تكنولوجيا المعلومات في جامعة الازهر سنة 2001 تحت مسمى "وحـدة تكنولوجيا المعلومات" بهدف وضع الخطط لإدارة كل ما يتعلـق بتكنولوجيـا المعلومـات فـي الجامعة.

تقوم وحدة تكنولوجيا المعلومات بصيانة أجهزة الحاسـوب وتوابعهـا، وحوسـبة الـدوائر الإدارية، وتطوير صفحة الإنترنت، توفير مختبرات الحاسـوب والإشـراف عليهـا لتـدريس المساقات التي تتعلق بالحاسوب الخاصة بالكليات، وعقد الدورات التدريبية في مجال الحاسوب، وتوفير خدمة الإنترنت والبريد الإلكتروني، تشرف وحدة تكنولوجيا المعلومات على ما يقـرب من 500 جهاز حاسوب موزعة على كليات ودوائر الجامعة(موقع جامعة الأزهر).

مجالات عمل وحدة تكنولوجيا المعلومات:

تقدم وحدة تكنولوجيا المعلومات الخدمات التكنولوجية في عدة مجالات (موقع جامعة الأزهـر) وهى:

1. **المجال الأكاديمي:** تعمل وحدة تكنو لوجيا المعلومات على تدريب الكادر الأكاديمي على استخدام التكنولوجيا الحديثة في العملية التعليمية، وكذلك تطوير الخدمات الأكاديمية مثل المكتبات الالكترونية.

2. **المجال الإداري:** تعمل وحدة تكنولوجيا المعلومات على حوسبة الأنظمة الإدارية لإدارة العملية الإدارية والأكاديمية مثل برامج: الدائرة المالية، وبرامج شئون الطلاب، وبرنامج دائرة اللوازم والمشتريات، وبرامج المكتبة المركزية، وبرامج التحاليل الطبية وغيرها.

3. **المجال الخدماتي:** تقوم وحدة تكنولوجيا المعلومات بتقديم الخدمات التالية:
   - تطوير أجهزة الحاسوب وملحقاتها وتوفير خدمات الصيانة لهذة الاجهزة.
   - توفير خدمات الانترنت والبريد الالكتروني للطلبة والموظفين.

هيكلية وحدة تكنولوجيا المعلومات:

تتكون وحدة تكنولوجيا المعلومات في جامعة الأزهر من ثلاث أقسام رئيسية (موقع جامعة الأزهر) وهي:

1. **قسم الصيانة:**

يقوم قسم الصيانة بصيانة جميع أجهزة الحاسوب وتوابعها، ووضع التوصيف الفني لأجهزة الحاسوب وتوابعها (طابعات، شاحن UPS، ماسحات ضوئية Scanner ،... إلخ، ويقوم بعملية التطوير لهذة الأجهزة بشكل مستمر لتواكب التطور التقني ولتلبي احتياجات العمل.

2. **قسم البرمجة.**

يقوم قسم البرمجة بانتاج وتصميم برمجيات الحاسوب الخاصة بدوائر الجامعة لتلبي احتياجات دوائر وكليات الجامعة والقيام بتطويرها حسب تطور الأنظمة المعمول بها في الجامعة ومن ثم القيام بتدريب مستخدمي هذة البرامج للعمل عليها بكفاءة وفعالية.

وقد قام قسم البرمجة بحوسبة العديد من الأنظمة وتحويل العديد من الإجراءات الإدارية اليدوية إلى المحوسبة مثل: برنامج القبول والتسجيل، وبرنامج الشئون الإدارية، وبرنامج الدائرة المالية وبرامج شئون الطلاب، وبرنامج دائرة اللوازم والمشتريات، وبرامج المكتبة المركزية، وبرامج التحاليل الطبية حيث استخدمت أنظمة أوراكل وفيجوال بيسك لإنتاج هذة البرمجيات.

3. **قسم التدريب وخدمات الإنترنت.**

يقوم القسم بعملية التدريب المستمر لمستخدمي أجهزة الحاسوب لإستخدامها بالشكل الأمثل وكذلك عقد الدورات التدريبية التي تتعلق بتكنولوجيا المعلومات لتطوير الكادر الإداري والأكاديمي لمواكبة التطورات التقنية، ويقوم القسم بالإشراف على تصميم وتحديث صفحة الإنترنت الخاصة بالجامعة باستمرار ويعمل على توفير خدمة الإنترنت والبريد الإلكتروني وعمل حسابات لمستخدمي الحاسوب (طلبة وموظفين) على شبكة الجامعة.

قام الباحث بزيارة ميدانية لوحد تكنولوجيا المعلومات في جامعة الأزهر فهي تعتبر صغيرة من الناحية الفنية والإدارية مقارنة بمراكز تكنولوجيا المعلومات في الجامعات الاخرى حيث أنها لم ترتقي بعد إلى مسمى " مركز تكنولوجيا المعلومات" فهى وحدة تقوم على تـوفير الخـدمات الفنية لتكنولوجيا المعلومات او حتى وجود أقسام إدارية مستقلة برئيس قسم يشرف على إنتـاج وآداء هذة الأقسام وهذا مؤشر على عدم وضوح الرؤية في مجال تكنولوجيا المعلومـات لـدى المعنيين في الجامعة أو حتى لدى إدارة وحدة تكنولوجيا المعلومات.

ثالثاً: مركز مركز الحاسوب- جامعة الأقصى

وحدة البرمجة وقسم الصيانة هما النواة التي من خلالهما تم استحداث مركز الحاسـوب منذ عام 2002 وذلك نتيجة للتطور الهائل في مجال تكنولوجيا المعلومـات ولمواكبـة التقـدم العلمي في المجالات الاكاديمية ولتلبية متطلبات افتتاح تخصصات علمية جديدة فـي الجامعـة، فكان لا بد من استحداث مركز حاسوب قادر على تقديم الخدمات التكنولوجية كالإنترنت والبريد الإلكتروني وحوسبة أنظمة دوائر وكليات الجامعة، فمركز الحاسوب هو الجهة التي من خلالها يتم ادخال التكنولوجيا الحديثة إلى الجامعة وتطوير الأساليب التعليمـة باسـتخدام التكنولوجيـا الحديثة، فهو العصب الرئيس في الجامعة لتطوير تكنولوجيا المعلومات فـي الجامعـة لخـدمو العملية الاكاديمية و المستويات الإدارية (موقع جامعة الأقصى).

يقوم مركز الحاسوب بالإشراف على جميع ما يتعلق بتكنولوجيا المعلومات في فـروع الجامعة الأخرى وهي فرع تل الهوى، فرع خانيونس (طالبـات)، فـرع خـانيونس(طـلاب) بالإضافة إلى الفرع الرئيسي، حيث يتوفر فنيي تابعيين لمركز الحاسوب للإشراف الفني علـى كل ما يتعلق بتكنولوجيا المعلومات في هذة الفروع.

مجالات عمل مركز الحاسوب:

يقوم مركز الحاسوب في جامعة الأقصى بتقديم الخدمات المتعلقة بتكنولوجيا المعلومات في عدة مجالات (موقع جامعة الأقصى) وهي:

1. **المجال الإداري:** يقوم مركز الحاسوب بحوسبة الأنظمة الإدارية لدوائر وكليات الجامعة مثل برامج: : برنامج القبول والتسجيل، برنامج الشئون الأكاديميـة، برنـامج شـئون الطلاب، برنامج شئون الموظفين، برنامج المخـازن والمـشتريات، برنـامج الـشئون الإدارية وغيرها.

2. **المجال الخدماتي:** يقوم مركز الحاسوب بتوفير خدمات الإنترنت والبريد الإلكتروني للطلبة والموظفين على حدٍ سواء وكذلك إمكانية الوصول إلى شبكة الحاسوب للمستخدمين (عمل حساب على شبكة الحاسوب خاص بكل مستخدم) وصيانة وتطوير أجهزة الحاسوب وملحقاتها.

- **هيكلية مركز الحاسوب.**

يتكون هيكلية مركز الحاسوب لجامعة الأقصى من ثلاث أقسام رئيسية (دليل جامعة الأقصى 2005-2006) وهي:

1. **قسم نظم المعلومات.**

هو القسم الذي يشرف على قاعدة البيانات في مركز الحاسوب وهو الذي يقوم بحوسبة الأنظمة الإدارية في الجامعة، ولخدمة المستويات الإدارية المختلفة، فهو يعمل على تحليل أنظمة الحاسوب المطلوبة للدوائر وبناء النظام الذي يناسب كل دائرة و من ثم يقوم بتدريب الموظفين الذين يستخدمون هذة البرامج، وقسم نظم المعلومات هو القسم الذي يقوم بالمحافظة على أمن البيانات وسريتها.

وقد قام القسم بانتاج عدة برامج لحوسبة الدوائر الإدارية المختلفة مثل: نظام القبول والتسجيل، النظام المالي، نظام الشئون الأكاديمية، نظام شئون الطلاب، نظام شئون الموظفين، نظام المخازن والمشتريات، نظام الشئون الإدارية، نظام المكتبة، نظام البطاقات الممغنطة للطلاب والموظفين والمكتبة، نظام الجودة، ونظام الخدمات الالكترونية الخاص بالموظفين والطلاب.

2. **قسم الشبكات والإنترنت.**

هو القسم الذي يعمل على توفير خدمة الإنترنت والبريد الإلكتروني وهو الذي يقوم بتصميم وتوسيع شبكة الحاسوب في الجامعة لتلبي الاحتياجات امطلوبة في ظل التطور التكنولوجي المتسارع في مجال تكنولوجيا المعلومات، وكذلك يقوم بربط جميع أفرع الجامعة بشبكة الحاسوب الرئيسية للجامعة لاسلكياً.

يقوم قسم الشبكات والإنترنت ببناء وتشغيل ومراقبة شبكة الحاسوب الداخلية -داخل الجامعة- وشبكة الحاسوب الرابطة بين أفرع الجامعة أيضا، علية فهو القسم الذي يقوم بتطوير أنظمة شبكة الحاسوب والإشراف على الخوادم الرئيسية Servers لشبكة الحاسوب في الجامعة وربطها بالإنترنت ومراقبة الشبكة من الإختراقات الخارجية والعمل على حماية البيانات الداخلية من الكشف نتيجة الإختراقات.

3. قسم الدعم الفني والمتابعة.

يقوم قسم الدعم الفني بصيانة أجهزة الحاسوب وملحقاتها، وكذلك يقو بالتوصيف الفني لأجهزة الحاسوب وملحقاتها لتلبية الإحتياجات المطلوبة في ظل التطور السريع في مجال تكنولوجيا المعلومات واعلمل على تحديث الأجهزة بشكل مستمر لتواكب التطور التكنولوجي ولتلبية احتياجات الدوائ والكليات المعنية، يقومم فنيي القسم بمساعدة مستخدمي أجهزة الحاسوب على حل المشاكل المتعلقة بالحاسوب التي تواجهم أثناء عملهم، ويقوم بالإشراف فنياً على مختبرات الحاسوب في الجامعة لإصلاح أي خال في جهاز الحاسوب لسير العملية التعليمية بشكل سليم.

تتكون شبكة الحاسوب في المقر الرئيس في جامعة الأقصى من 14 خادم (Server) و28 موزع شبكة(Switch/Hub) وبسرعة تراسل 10/100Mbps، وهناك إحصائيات حول الشبكة تم الحصول عليها نتيجة المقابلات الشخصية مع مدير شبكة الحاسوب في المركز والتي تخص المقر الرئيس للجامعة فقط (مدير شبكة الحاسوب- جامعة الأقصى) كما هو موضح في الجدول (3-5):

جدول (3-5) إحصائيات شبكة الحاسوب والأجهزة المتصلة بها في جامعة الأقصى

البند	العدد
نقاط الشبكة	350
مشتركي خدمة البريد الإلكتروني	398
مشتركي خدمة الإنترنت داخل الجامعة	859
موزعات الشبكة	28
عدد الأجهزة المركزية Servers	14
أجهزة الحاسوب	277

رابعاً: مركز تكنولوجيا المعلومات والإتصالات –جامعة القدس المفتوحة.

تكنولوجيا المعلومات تلعب دوراً رئيسساً في العملية الأكاديمية لجامعة القدس المفتوحة، حيث ان إدارة الجامعة تدعم بيئة التعليم الإلكتروني حيث يوجد لها 20 فرعاً منتشرة في ربوع مناطق السلطة الفلسطينية في محافظات الضفة الغربية وقطاع غزة والقدس الشرقية موزعة ما بين مركز دراسي ومنطقة تعليمية مرتبطة معاً بشبكة حاسوب (موقع جامعة القدس المفتوحة) ، لذلك وبالنظر إلى الهيكلية التنظيمية لتكنولوجيا المعلومات نجد أن مدير مركز

تكنولوجيا المعلومات والإتصالات يتبع مباشرة رئيس الجامعة وذلك لأهميـة التكنولوجيـا فـي العملية التعليمية بشكل خاص بالنسبة لجامعة القدس المفتوحة (موقع جامعة القدس المفتوحة).

يهـدف مركـز تكنولوجيـا المعلومـات والاتـصالات (Information & Communications Technology Center - ITTC) إلى توفير البنية التحتية لتكنولوجيـا المعلومات وذلك من خلال ايجاد البنية التحتية لشبكة حاسوب قـادرة علـى تـوفير الخـدمات الإلكترونية لجميع فروع الجامعة في كافة المناطق وكذلك حوسبة كافـة المـستويات الإداريـة والأكاديمية لتلبية احتياجات العملية الأكاديمية والإدارية تساعد فـي غـدارة وتنفيـذ البـرامج الاكاديمية لخدمة العملية التعليمية في جميع فروع الجامعة المتباعدة، لذلك تعمل الجامعة علـى تعزيز بيئة التعليم الإلكتروني ليكون فعالاً في العملية التعليمية، لذلك يقـوم مركـز تكنولوجيـا المعلومات والإتصالات بتدريب موظفي الجامعة بشكل مستمر على استخدام التكنولوجيا الحديثة لإنجاز المهام الموكله إليهم.

- **مهام مركز تكنولوجيا المعلومات والاتصالات ICTC:**

يقوم مركز تكنولوجيا المعلومات والإتصالات (موقع جامعة القدس المفتوحة) بالمهام التالية:

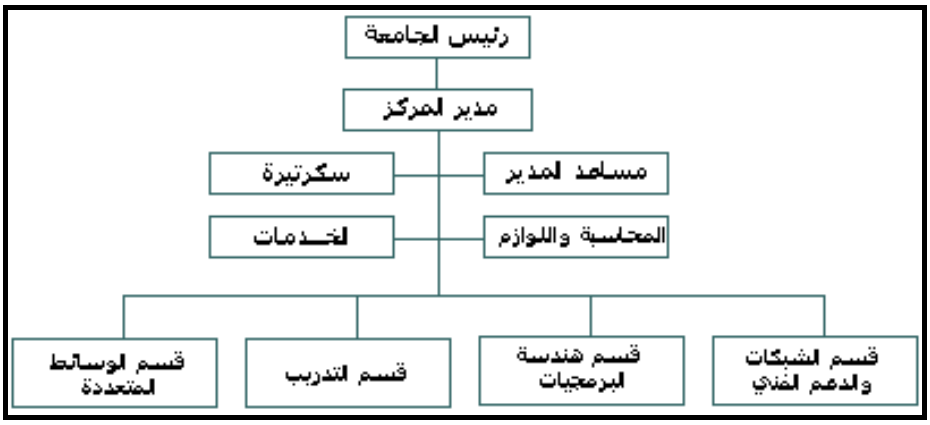
1. إنشاء شبكة حاسوب محلية في كل فرع للجامعة وربط جميع هذة الشبكات معاً لتـشكل شبكة حاسوب موحدة تربط جميع أفرع الجامعة في المناطق.
2. توفير خدمة الإنترنت والبريد الإلكتروني والوصول بالجامعة لتكون مزود خدمة إنترنت مستقلة بذاتها (Self Service Provider).
3. تصميم صفحة الإنترنت وتحديثها بشكل متواصل.
4. العمل على حوسبة جميع الأنظمة المالية والإدارية وتطـوير الأنظمـة المحـوسـبة المعمول بها حالياً في الجامعة لتلبي احتياجات العمل.
5. العلم على حوسبة الشؤون الأكاديمية (أي العملية التعليمية) وذلك باستخدام التكنولوجيـا بشكل كامل في العملية التعليمية وتعزيز التعليم الإلكتروني في العملية التعليمية او فـي التعليم الذاتي .
6. إنشاء مكتبة إلكترونية وربطها بالجامعات المحلية والعالمية وتكـوين بنـك معلومـات للأبحاث يكون متاحاً للجميع مما يفيد البحث العلمي والباحثين في كافة المجالات.
7. القيام بجميع أعمال الصيانة الفنية والسريعة لجميع أجهـزة الحاسـوب والمعـدات ذات العلاقة بتكنولوجيا المعلومات في جميع مراكز الجامعة ومناطقها التعليمية.
8. الاتصال بالجهات المانحة لتوفير الدعم المـالي لتطـوير البنيـة التحتيـة لتكنولوجيـا المعلومات في مراكز الجامعة.

- **الهيكل التنظيمي لمركز تكنولوجيا المعلومات والاتصالات ITTC**

تتكون هيكلية مركز تكنولوجيا المعلومات والإتصالات لجامعة القدس المفتوحة من مدير المركز ومساعد وأربعة أقسام رئيسية هي:

1. قسم الشبكات و الدعم الفني
2. قسم هندسة البرمجيات
3. قسم التدريب
4. قسم الوسائط المنعددة

وحيث أن المقر الرئيس للمركز يقع فى منطقة القدس بينما المقر الموجود قي قطاع غزة إنما يعتبر فرع للمركز الرئيس يقوم بالإشراف مختبرات الحاسوب و المهام الفنية التي يمكن أن تعترض سير العملية التعليمية فى أفرع الجامعة في قطاع غزة.



(شكل 5-3) الهيكل التنظيمي لمركز تكنولوجيا المعلومات والاتصالات لجامعة القدس المفتوحة (موقع جامعة القدس المفتوحة)

مشرف تكنولوجيا المعلومات في قطاع غزة هو المسؤول المباشر على جميع الموظفي التابعين لمركز تكنولوجيا المعلومات في قطاع غزة والذي يكون تابعاً مباشراً لمدير مركز تكنولوجيا المعلومات والاتصالات ITTC الرئيس الموجود في القدس.

رأي الباحث:

قام الباحث بزيارات ميدانية لجميع مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، وقد قام الباحث بمقابلة جميع رؤوساء أقسام المراكز والإطلاع على سير العمل في هذه المراكز فقد وجد الباحث انها تقوم بتوفير االخدمات الفنية التي يجب أن يقوم بتوفيرها أي مركز لتكنولوجيا المعلومات للمستخدمين من إنترنت وبريد إلكتروني،...إلخ بينما لا نجد لهذه المراكز دور مميز في تنمية المجتمع أو طرح مشاريع إبداعية لتنفيذها في مجال تكنولوجيا المعلومات أو طرح مشاريع تكنولوجية مميزة تفيد مركز تكنولوجيا المعلومات أو المجتمع ويعتقد الباحث أن السبب في ذلك يرجع إلى عدم وجود خطط تنموية لدى إدارة مراكز تكنولوجيا المعلومات وإلى عدم وضوح الهدف الذي تسعى إلى تحقيقه ليساهم في مثل هذة الأبحاث أو المشاريع، في حين أننا نجد لها اهتمام كبير في إنتاج البرامج المطلوبة للدوائر والكليات وذلك للحاجة الملحة لهذه الدوائر في رفع مستوى الأداء لديها وانجاز أعمالها بإتقان، كذلك بالنسبة لتوصيف أجهزة الحاسوب وملحقاتها والإهتمام الكبير بمختبرات الحاسوب وتطويرها وذلك بسبب العملية التعليمية التي تحتاج إلى أجهزة متطورة باستمرار وهذا ضمن الخدمات التي تقوم بتوفيرها.

لم يجد الباحث خطة إستراتيجة لهذة المراكز التي تكون كالمنارة التي يسعى كل مركز للوصول إليها مما له انعكاس مباشر على أمن المعلومات في مراكز تكنولوجيا المعلومات، وهذا يعني أنه لا يوجد رؤية تكنولوجية واضحة لإدارة هذة المراكز إلى الهدف التي تسعى إلى تحقيقة، وبالتالي يعتقد الباحث أنه نتيجة لعدم خطة استراتيجية لمركز تكنولوجيا المعلومات فإنه بالتأكيد لن يكون هناك خطة استراتيجية لأمن المعلومات في المركز حيث أن الباحث لم يقابل أي موظف في مراكز تكنولوجيا المعلومات متخصص بأمن المعلومات ذات مسمى وظيفي مدير أمن المعلومات (Security Administrator).

مراكز تكنولوجيا المعلومات في الجامعات تعتبر البوابة التي من خلالها يتم إدخال التكنولوجيا الحديثة إلى الجامعات وتطويرها بشكل مستمر لتواكب التطور العلمي والتكنولوجي المتسارع لتسخيره في خدمة العملية التعليمية والمضي بها قدما، لذلك فهذه المراكز بحاجة إلى تقييم مستمر من قبل القائمين عليها وبحاجة أيضاً إلى متابعة لهذه المراكز من قبل الإدارة العليا للجامعة لتكون مرجع علمي وتكنولوجي ولتقديم الاستشارات لجميع المهتمين والمتخصصين والمراكز والشركات ذو العلاقة بتكنولوجيا المعلومات في قطاع غزة.

الفصل الرابع

منهجية الدراسة

أولاً: منهجية الدراسة

ثانياً: مصادر جمع المعلومات

ثالثاً: أداة الدراسة

رابعاً: مجتمع الدراسة

خامساً: عينة الدراسة

سادساً: صدق و ثبات الاستبيان

سابعاً: المعالجات الإحصائية

الفصـــل الرابع
المنهجية والإجراءات

مقدمة:

هدفت هذة الدراسة إلى التعرف على متطلبات استخدام التوقيع الإلكترونـي فـي إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، حيث يتناول هذا الفـصل المنهجية التي تم اتباعها في اختيار العينة من الأفراد مجتمـع الدراسـة، كـذلك أداة الدراسـة المستخدمة في هذه الدراسة وبيان مدى صدقها وثباتها باستخدام طرق متعددة، ثم بيان الأساليب الإحصائية التي تم استخدامها في هذه الدراسة، كذلك يتضمن هذا الفصل وصفاً للإجراءات التي استخدمت في تقنين أدوات الدراسة وتطبيقها، والمعالجات الإحصائية التي تم اعتمادها في تحليل الدراسة.

4.1 منهجية الدراسة:

لتحقيق أهداف الدراسة تم استخدام المنهج الوصفي التحليلي "وهو المنهج الـذي يعتمـد على دراسة الواقع ويهتم بوصفها وصفاً دقيقاً ويعبر عنها تعبيـراً كيفيـاً أو كميـاً"، عبيـدات 2006)، ويعتبر هذا المنهج مناسباً لهذه الدراسة لأنه يقوم على جمع البيانـات للتعـرف علـى متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيـا المعلومـات فـي الجامعـات الفلسطينية في قطاع غزة، وقد تم الحصول علـى البيانـات اللازمـة مـن خـلال الاسـتبانة (Questionnaire) التي تم إعدادها لهذا الغرض، وتـم تفريـغ البيانـات وتحليـل النتـائج باستخدام البرنامج الإحصائي SPSS (Statistical Package for Social Science)

4.2 مصادر جمع المعلومات :

أولاً: المصادر الثانوية:

تم استخدام العديد من المصادر الثانوية في الدراسة الحالية وتمثلت في :

- النشرات والإحصائيات التي لها علاقة بموضوع البحث .
- الكتب والدوريات والمجلات الأجنبية .

- الدراسات والبحوث العلمية والتكنولوجية التي لها علاقة بموضوع البحث .
- شبكة الإنترنت .

ثانياً: المصادر الأولية وتمثلت في الاستبانة لجمع البيانات والمعلومات اللازمـة عـن مجتمـع الدراسة ومعالجتها وتحليلها إحصائياً والحصول على النتائج.

4.3 أداة الدراسة:

تم استخدام "الاستبانة" لتحقيق أهداف الدراسة حيث تم تصميم فقرات الاسـتبانة حـسب الخطوات التالية:

تم تحديد الهدف الذي من أجله ستصمم الاستبانة وهو التعرف على متطلبات استخدام التوقيـع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، وقد كانت إجابات كل فقرة وفق مقياس ليكارت الخماسي كالتالي:

التصنيف	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الترميز	5	4	3	2	1

وصف الاستبيان بعد التقنين:

تكون الاستبيان من قسمين هما:

أولاً: المعلومات العامة لعينة الدراسة ومدى استخدامها للتوقيع الإلكتروني ومتطلباته، ويتكـون من 14 فقرة.

ثانياً: مجالات الدراسة: وتتكون من خمس مجالات تحتوي على (32) فقرة وهم كالتالي:

المجال الأول : تطوير البنية التحتية لمركز تكنولوجيا المعلومات، ويتكون من 7 فقرات.

المجال الثاني : اهتمام الإدارة العليا لمركز تكنولوجيا المعلومات باستخدام التوقيع الإلكترونـي، ويتكون من 9 فقرات.

المجال الثالث : وجود المتطلبات القانونية والتشريعية لاستخدام التوقيع الإلكتروني، ويتكون من 5 فقرات.

المجال الرابع: اعتماد المراسلات الإلكترونية، ويتكون من 5 فقرات.

المجال الخامس: سياسات حماية المعلومات، ويتكون من 6 فقرات

مجتمع الدراسة:

يتكون مجتمع الدراسة من جميع العاملين في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وذلك على اعتبار أن هذة الفئة من العاملين على اطلاع مستمر بالتطور التكنولوجي وهي الفئة الأكثر وعياً بتفاصيل العمل وتستطيع اتخاذ القرارات كلٌ في مجال عمله وتقديم التوصيات للإدارة العليا للجامعات الفلسطينية في قطاع غزة، فهذه الفئة المتخصصة تستطيع الإجابة على فقرات الاستبانة دون غيرها من الفئات الأخرى الغير متخصصة والغير مطلعة على التطورات التكنولوجية، ويبلغ حجم مجتمع الدراسة (74) موظفاً ويبلغ عدد الجامعات قيد الدراسة أربعة جامعات من أصل خمسة وذلك ان جامعة فلسطين قيد البناء والبنية التحتية لشبكة الحاسوب قيد الإنشاء وحتى لا تؤثر على نتائج الدراسة فقد تم استبعادها والجامعات هى:

- الجامعة الإسلامية
- جامعة الأزهر
- جامعة الأقصى
- جامعة القدس المفتوحة

وقد تم الحصول على البيانات حول عدد موظفي مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية من خلال دائرة شؤون الموظفين التابعة لكل جامعة.

جدول رقم (4.1)

عدد موظفي مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة

#	اسم الجامعة	عدد الموظفين العاملين في مراكز تكنولوجيا المعلومات
1	الجامعة الإسلامية	35
2	جامعة الأزهر	13
3	جامعة الأقصى	12
4	جامعة القدس المفتوحة- غزة	14
المجموع		**74**

عينة الدراسة :

تشمل الدراسة جميع العاملين في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية أي تم استخدام اسلوب الحصر الشامل نظراً لقلة العدد وسهولة الوصول إلى جميع أفراد العينة حيث كانت عينة الدراسة (74) موظف، وقد تم توزيع الاستبانات عليهم، وقد تم استرداد (65) استبانة، وبعد تفحص الاستبانات تم استبعاد (7) استبانات لعدم جدية الإجابة عليهم او بسبب المؤهل العلمي أقل من ثانوية عامة وعدم تحقيق الشروط المطلوبة للإجابة على الاستبيان، وبذلك يكون عدد الاستبانات الخاضعة للدراسة (58) استبانة أي ما يعادل نسبة (78%) من المجتمع الكلي للدراسة، والجداول التالية توضح ذلك .

والجداول التالية تبين خصائص عينة الدراسة كالتالي:

جدول (4.2)

عدد أفراد عينة الدراسة حسب الجامعة

الجامعة	العدد المستهدف	العدد المسترد	العدد الصالح للتحليل	النسبة المئوية
الإسلامية	35	34	27	46.55
الأزهر	13	11	11	18.97
الأقصى	12	11	12	20.69
القدس المفتوحة	14	9	8	13.79
المجموع	**74**	**65**	**58**	**100.00**

يبين جدول رقم (4.2) أن ما يعادل 46.55% من عينة الدراسة من الجامعة الإسلامية و18.97% من جامعة الأزهر و20.69% من جامعة الأقصى و13.79% من جامعة القدس المفتوحة، حيث ان عينة الدراسة تشمل جميع فروع الجامعات.

جدول (4.3)

عدد أفراد عينة الدراسة حسب المؤهل

المؤهل	العدد	النسبة المئوية
دبلوم	14	24.14
بكالوريوس	39	67.24
دراسات عليا	5	8.62
المجموع	**58**	**100.00**

يبين جدول رقم (4.3) أن 8.62% من عينة الدراسة يحملون مؤهل الدراسات عليا ويعزو الباحث إلى انخفاض نسبة أفراد العينة ذات المؤهل "دراسات عليا" إلى أن طبيعة العاملين في هذة المراكز هم موظفين إداريين فنيين وليس أكاديميين ولا تحتاج إلى شهادات عليا بقدر احتياجاتهم إلى خبرة عملية في مجال العمل.

جدول (4.4)

عدد أفراد عينة الدراسة حسب التخصص

التخصص	العدد	النسبة المئوية
هندسة حاسوب	12	20.69
علوم كمبيوتر	35	60.34
تكنولوجيا معلومات	11	18.97
المجموع	**58**	**100.00**

يبين الجدول رقم (4.4) أن 60.34% من عينة الدراسة علوم كمبيوتر، ويعزو الباحث إرتفاع نسبة أفراد العينة تخصص " علوم كمبيوتر" ، إلى أن كليات العلوم في الجامعات الفلسطينية تم إفتتاحها قبل كليات الهندسة وبذلك تكون نسبة المتقدمين للوظيفة من خريجي كلية العلوم أعلى منها من أي كلية أخرى.

جدول (4.5)

عدد أفراد عينة الدراسة حسب عمر مركز تكنولوجيا المعلومات

عمر مركز تكنولوجيا المعلومات	العدد	النسبة المئوية
سنتان-5 سنوات	11	27.69
6-10 سنوات	36	55.38
أكثر من 10 سنوات	11	16.92
المجموع	**58**	**100.00**

الجدول رقم (4.5) يوضح أن 55.38% من عينة الدراسة يعملون في مراكز تكنولوجيا معلومات ذات عمر من (6- 10 سنوات) وهى النسبة الأعلى مقارنة بعمر المراكز الأخرى ويعزو الباحث ذلك إلى أن مراكز تكنولوجيا المعلومات قد تم إنشاءها في فترة متأخرة من إنشاء الجامعة حيث كان ذلك في عقد التسعينات.

جدول (4.6)

عدد أفراد عينة الدراسة حسب سنوات الخبرة

عدد سنوات الخبرة	العدد	النسبة المئوية
أقل من سنتين	1	1.72
سنتان-5 سنوات	29	50.00
سنوات6-10	23	39.66
أكثر من 10 سنوات	5	8.62
المجموع	**58**	**100.00**

يبين جدول رقم (4.6) أن50.00% من عينة الدراسة تمتلك خبرة (من سنتين – 5 سنوات) ويعزو الباحث إرتفاع هذة النسبة إلى ان نسبة كبيرة من موظفي هذة المراكز قد تم توظيفهم في السنوات الخمس الأخيرة، بينما نجد أن عدد أفراد العينة ذات خبرة أكثر من 10 سنوات (8.62%) هم الفئة الأقل وذلك يرجع إلى أن مراكز تكنولوجيا المعلومات قد تم إنشاءها في فترات متأخرة بعد إنشاء الجامعة وهذا يتوافق مع نتيجة الجدول رقم (4.5).

جدول (4.7)

عدد أفراد عينة الدراسة حسب المسمى الوظيفي

المسمى الوظيفي	العدد	النسبة المئوية
رئيس المركز	3	5.17
مدير دائرة	2	3.45
رئيس قسم	7	12.07
مدير شبكة	3	5.17
صيانة حاسوب ودعم فني	32	55.17
محلل نظم	2	3.45
مصمم صفحات إنترنت	3	5.17
مبرمج	6	10.34
المجموع	**58**	**100.00**

يبين جدول رقم (4.7) أن 5.17% من عينة الدراسة المسمى الوظيفي "رئيس مركز تكنولوجيا المعلومات "، و 3.45% من عينة الدراسة المسمى الوظيفي مدير دائرة، 12.07% المسمى الوظيفي رئيس قسم، المسمى الوظيفي مدير قواعد بيانات، و 5.17% من عينة الدراسة المسمى الوظيفي مدير شبكة حاسوب، و 55.17% من عينة الدراسة المسمى الوظيفي صيانة حاسوب ودعم فني، و 3.45% من عينة الدراسة المسمى الوظيفي محلل نظم، و5.17% من عينة الدراسة المسمى الوظيفي مصمم صفحات إنترنت، و 10.34% من عينة الدراسة المسمى الوظيفي مبرمج، بينما مسميات وظيفية" مدير أمن معلومات " و " مدير قواعد بيانات" و" مدير أنظمة تشغيل" غير متوفرة في جميع مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة.

تقنين الاستبيان:

تم تطبيق الاستبيان على عينة استطلاعية بلغت (20) موظفاً من العاملين في مراكز تكنولوجيا المعلومات في بالجامعات الفلسطينية في قطاع غزة بهدف:

1. حساب معامل الصدق .
2. حساب معامل الثبات .

أولاً: حساب معامل الصدق Validity Coefficient:

تم حساب صدق الاستبيان بعدة طرق منها:

1- صدق المحكمين:

تم عرض الاستبيان في صورته المبدئية على مجموعة من المحكمين تألفـت مـن (8) أعضاء من الأساتذة والمختصين في تكنولوجيا المعلومات وإدارة الأعمال والتحليل الإحـصائي للتأكد من سلامة الاستبيان في كافة النواحي، وقام الباحث بحذف وتعديل الفقرات التي أشار إليها المحكمون، وقد قُبلت الفقرات إذا وافق عليها أكثر من (6) محكمين، وعدلت إذا وافـق عليهـا أكثر من (4-6) محكمين، ورفضت إذا وافق عليها أقل من (3) محكمين ولقد كان الاستبيان في صورته الأولية يتكون من (56) فقرة تم حذف (10) منها بناء على رغبة الـسادة المحكمـين حيث أصبح في صورته النهائية (46) فقرة.

2- حساب الاتساق الداخلي (اختبار بيرسون):

لقد أجرى الباحث الاستبيان المعد في صورته النهائية على العينة الاسـتطلاعية حيـث شملت على (20) موظـف، حيـث قـام بمعالجـة البيانـات وتحليلهـا باسـتخدام الرزمـة الإحصائية SPSS وقد تم حساب معامل الارتباط بين كل فقرة من فقرات الاستبيان مع الدرجـة الكلية للمجال الذي ينتمي إليه والجداول التالية توضح ذلك:

جدول (4.8)

معاملات الارتباط بين كل فقرة من فقرات المجال الأول مع الدرجة الكلية للمجال

الفقرة	معامل الارتباط	مستوى الدلالة
يستخدم مركز تكنولوجيا المعلومات تقنيات بديلة عن التوقيع الإلكتروني؟	0.510	دالة عند 0.05
موازنة مركز تكنولوجيا المعلومات تسمح بإنـشاء بنيـة تحتيـة لتقنيـة التوقيـع الإلكتروني	0.753	دالة عند 0.01
يدرك موظفو مركز تكنولوجيا المعلومات بأهمية استخدام التوقيع الإلكتروني	0.547	دالة عند 0.05
المعدات الأمنية المستخدمة في مركز تكنولوجيا المعلومـات لحمايـة المراسـلات الإلكترونية تواكب التطور التقني	0.547	دالة عند 0.05
البرمجيات الأمنية المستخدمة في مركز تكنولوجيا المعلومات لحمايـة المراسـلات الإلكترونية يتم تحديثها بشكل مستمر	0.856	دالة عند 0.01
موظفو مركز تكنولوجيا المعلومات على إطلاع مـستمر بتطـور تقنيـات أمـن المعلومات بشكل عام وبتقنية التوقيع الإلكتروني بشكل خاص	0.733	دالة عند 0.01
موظفو مركز تكنولوجيا المعلومات يمتلكون مؤهلات وخبرات تقنية جيدة في إنشاء تقنيات أمن المعلومات وخاصة تقنية التوقيع الإلكتروني	0.820	دالة عند 0.01

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.05) = 0.444

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.01) = 0.561

جدول رقم (4.8) يبين الارتباط بين كل فقرة من فقرات المجال الأول (تطـوير البنيـة التحتية لمركز تكنولوجيا المعلومات) والدرجة الكلية لفقراته، حيث كانت معـاملات الارتبـاط محصورة بين المدى (0.510 و 0.856)، وهي قيم دالة عند الارتباط المبينة دالة عند مستوى دلالة (0.05، 0.01)، وبذلك تعتبر فقرات المجال الاول صادقة لما وضعت لقياسه.

جدول (4.9)

معاملات الارتباط بين كل فقرة من فقرات المجال الثاني مع الدرجة الكلية للمجال

الفقرة	معامل الارتباط	مستوى الدلالة
استخدام تقنية التوقيع الإلكتروني مدرجة ضـمن الخطـة الإسـتراتيجية لمركز تكنولوجيا المعلومات	0.736	دالة عند 0.01
تعمل إدارة مركز تكنولوجيا المعلومات على إنشاء البنية التحتيـة لتقنيـة التوقيع الإلكتروني	0.486	دالة عند 0.05
إدارة مركز تكنولوجيا المعلومات على اطلاع مستمر بالتطورات التقنيـة لأمن المعلومات	0.761	دالة عند 0.01
إدارة مركز تكنولوجيا المعلومات على إطلاع بأهمية اسـتخدام التوقيـع الإلكتروني	0.790	دالة عند 0.01
إدارة مركز تكنولوجيا المعلومات حريصة على تطوير موظفي المركـز بصورة مستمرة في مجال آمن المعلومات	0.719	دالة عند 0.01
تعتمد إدارة مركز تكنولوجيا المعلومات المراسلات الإلكترونية	0.504	دالة عند 0.05
تعتمد إدارة مركز تكنولوجيا المعلومات الشهادات الرقمية للخادم الرئيسي في المركز وللمراسلات الإلكترونية	0.446	دالة عند 0.05
تعمل إدارة مركز تكنولوجيا المعلومات ضمن خطة إستراتيجية واضحة	0.614	دالة عند 0.01
إدارة مركز تكنولوجيا المعلومات قادرة على إدارة المركز بكفاءة	0.759	دالة عند 0.01

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.05) = 0.444

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.01) = 0.561

جدول رقم (4.9) يبين معاملات الارتباط بين كل فقرة من فقـرات المجـال الثـاني والدرجة الكلية لفقراته، والذي يبين أن معاملات الارتباط المبينة والتي تنحصر بين (0.446 و 0.790) دالة عند مستوى دلالة (0.05، 0.01)، وبذلك تعتبر فقرات المجال الثاني صـادقة لما وضعت لقياسه.

جدول (4.10)

معاملات الارتباط بين كل فقرة من فقرات المجال الثالث مع الدرجة الكلية للمجال

الفقرة	معامل الارتباط	مستوى الدلالة
يلزم استصدار تشريع قانوني من المجلس التشريعي يسمح باستخدام التوقيع الإلكتروني بين دوائر الجامعة	0.731	دالة عند 0.01
استخدام التوقيع الإلكتروني بين أقسام ودوائر الجامعة بحاجة إلى موافقة الإدارة العليـا للجامعة	0.691	دالة عند 0.01
يعتمد استخدام التوقيع الإلكتروني في المراسلات الإلكترونية بين أقسام مركز تكنولوجيا المعلومات بأخذ موافقة إدارة المركز	0.679	دالة عند 0.01
التوقيع الإلكتروني بحاجة إلى استصدار قانون تشريعي من المجلس التشريعي لحمايته	0.808	دالة عند 0.01
إبرام العقود الإلكترونية يتم حمايتها قانونياً وتشريعياً	0.778	دالة عند 0.01

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.05) = 0.444

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.01) = 0.561

جدول رقم (4.10) يبين معاملات الارتباط بين كل فقرة من فقـرات المجـال الثالـث والدرجة الكلية لفقراته، والذي يبين أن معاملات الارتباط المبينة والتي تنحصر بـين (0.679 و 0.808) دالة عند مستوى دلالة (0.01)، وبذلك تعتبر فقرات المجال الثالث صادقة لما وضعت لقياسه.

جدول (4.11)

معاملات الارتباط بين كل فقرة من فقرات المجال الرابع مع الدرجة الكلية للمجال

الفقرة	معامل الارتباط	مستوى الدلالة
يتم تبادل المراسلات الإلكترونية بين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعة إلكترونياً	0.571	دالة عند 0.01
يتم تبادل المراسلات إلكترونياً بين أقسام المركز	0.827	دالة عند 0.01
تستخدم تقنية التوقيع الإلكتروني في المراسلات الإلكترونية لمركز تكنولوجيا المعلومات	0.685	دالة عند 0.01
تتوفر الإمكانيات التقنية في مركز تكنولوجيا المعلومات لحفظ واعتماد المراسلات الإلكترونية	0.587	دالة عند 0.01
اعتماد المراسلات الإلكترونية بين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعـة بحاجة إلى اعتماد الإدارة العليا للجامعة	0.539	دالة عند 0.05

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.05) = 0.444

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.01) = 0.561

جدول رقم (4.11) يبين معاملات الارتباط بين كل فقرة من فقرات المجال الرابع والدرجة الكلية لفقراته، والذي يبين أن معاملات الارتباط المبينة والتي تنحصر بين (0.539 و0.827) دالة عند مستوى دلالة (0.05، 0.01)، وبذلك تعتبر فقرات المجال الرابع صادقة لما وضعت لقياسه.

جدول (4.12)

معاملات الارتباط بين كل فقرة من فقرات المجال الخامس مع الدرجة الكلية للمجال

الفقرة	معامل الارتباط	مستوى الدلالة
1. يعتمد مركز تكنولوجيا المعلومات سياسات خاصة بآمن المعلومات	0.684	دالة عند 0.01
2. توجد سياسات خاصة باستخدام التوقيع الإلكتروني في مركز تكنولوجيا المعلومات	0.826	دالة عند 0.01
3. تعمل إدارة مركز تكنولوجيا المعلومات بصورة مستمرة على تطوير السياسات الخاصة بالتوقيع الإلكتروني	0.782	دالة عند 0.01
4. السياسة الأمنية المتبعة في مركز تكنولوجيا المعلومات تحقق سرية المعلومات	0.779	دالة عند 0.01
5. توجد سياسات خاصة بآمن المعلومات الإلكترونية معروفة لدى جميع الموظفين	0.700	دالة عند 0.01
6. يفتقد المركز إلى سياسة واضحة لحماية خصوصية المراسلات الإلكترونية	0.453	دالة عند 0.05

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.05) = 0.444

r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.01) = 0.561

جدول رقم (4.12) يبين معاملات الارتباط بين كل فقرة من فقرات المجال الخامس والدرجة الكلية لفقراته، والذي يبين أن معاملات الارتباط المبينة والتي تنحصر بين (0.453 و 0.826) دالة عند مستوى دلالة (0.05، 0.01)، وبذلك تعتبر فقرات المجال الخامس صادقة لما وضعت لقياسه.

يتضح من الجداول السابقة أن هناك اتساقاً داخلياً للفقرات مع الدرجة الكلية للمجال الذي ينتمي إليه، وعليه يصبح الاستبيان في صورته النهائية مكوناً من (32) فقرة والجدول التالي يوضح ارتباط كل مجال من مجالات الاستبيان مع الدرجة الكلية للاستبيان وكذلك كل مجال مع المجال الآخر.

الجدول (4.13)

ارتباط كل بعد من أبعاد الاستبيان مع الدرجة الكلية للاستبانة

المجال	الدرجة الكلية للاستبانة
الأول	0.830**
الثاني	0.793**
الثالث	0.475*
الرابع	0.603**
الخامس	0.750**

* r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.05) = 0.444

** r الجدولية عند درجة حرية (20-2) وعند مستوى دلالة (0.01) = 0.561

يتضح من الجدول (4.13) أن هناك ارتباطاً واتساقاً بين درجة كُل بعد والدرجة الكلية للاستبيان وعليه فإن الباحث يطمئن لصدق الاستبيان.

1- ثبات الاستبانة:

ويقصد بثبات الاستبانة أن تعطي الاستبانة النتائج نفسها تقريباً إذا أعيد تطبيقها على العينة نفسها مرة ثانية، ولقد قام الباحث بحساب معامل الثبات بطريقتين هما:

أ- طريقة التجزئة النصفية:

حيث تم تجزئة فقرات كل مجال من مجالات الاستبانة إلى جزأين الأسئلة التي تنتمي للنصف الأول والأسئلة التي تنتمي للنصف الثاني، ثم حساب معامل ارتباط بيرسون بين النصف الأول والنصف الثاني، وبعد ذلك تم تصحيح معامل الارتباط باستخدام معادلة سبيرمان براون.

الجدول (4.14)

عدد الفقرات لكل بعد وللاستبانة ككل ومعامل الارتباط قبل التعديل وبعد التعديل "الثبات"

البعد	عدد الفقرات	الارتباط قبل التعديل	الارتباط بعد التعديل "الثبات"
الأول	7	0.854	0.858
الثاني	9	0.501	0.566
الثالث	5	0.715	0.748
الرابع	5	0.705	0.743
الخامس	6	0.508	0.674
المجموع	**32**	**0.412**	**0.584**

يتضح من الجدول (4.14) أن معاملات الثبات تتـراوح مـا بـين (0.566 – 0.858) لمجالات الاستبانة أما الاستبانة ككل فكان معامل الثبات بعد التعديل (0.584) وهو معامل ثبات مقبول في مثل هذه الدراسات.

ب- طريقة ألفا كرونباخ:

حيث تم حساب الثبات بطريقة ألفا كرونباخ، حيث أن الجدول رقم (4.14) يبين معامل ألفا كرونباخ لكل بعد من الأبعاد و كذلك معامل ألفا للإستبانة ككل.

الجدول (4.15)

عدد الفقرات ومعامل ألفا كرونباخ لكل بعد وكذلك للاستبانة ككل

البعد	عدد الفقرات	معامل ألفا كرونباخ
الأول	7	0.807
الثاني	9	0.742
الثالث	5	0.784
الرابع	5	0.626
الخامس	6	0.730
المجموع	**32**	**0.873**

يتضح من الجدول (4.15) أن معاملات الثبات باستخدام معامل ألفا كرونباخ تراوحـت ما بين (0.626) لمجالات الاستبانة أما الاستبانة ككل فكان معامل ألفا كرونباخ (0.873) وهـو معامل ثبات عال في مثل هذه الدراسات.

وفي ضوء ما سبق نجد أن الصدق والثبات قد تحققا بدرجة عالية تطمئن الباحث لتطبيق الاستبانة على عينة الدراسة.

خطوات الدراسة الميدانية:

1- الدراسة الاستطلاعية:

قام الباحث بعمل دراسة استطلاعية على عينة مشابهة لمجتمـع البحـث قوامهـا (20) موظف من مراكز تكنولوجيا الجامعات الفلسطينية في قطاع غزة وذلك:

1. للتأكد من صدق وثبات الاستبانة على عينة البحث المختارة لموضوع البحث.
2. معرفة مدى ملاءمة الاستبانة لواقع وعينة البحث.
3. التعرف على المشكلات والمواقف التي قد يتعرض لها الباحث أثناء تطبيـق الاسـتبانة على عينة البحث.
4. وضع الحلول والتعديلات المطلوبة في حالة وجود ما يعترض الباحـث أثنـاء تطبيـق الأستبانة في الدراسة الاستطلاعية.
5. معرفة متوسط الزمن المتطلب للإجابة على الاستبانة.
6. الوصول إلى أنسب الطرق المنظمة لتحديد هيكل العمل المطلوب والقائم علـى توزيـع وجمع الاستبانة وتنفيذ الاستبانة بدقة وسهولة ويسر على عينة البحث.

2- تطبيق البحث:

طبق الباحث الاستبانة في صورة مطبوعة تم توزيعها على المـوظفين فـي الجامعـات الفلسطينية في محافظة غزة، وقام الباحث بشرح هدف البحث للموظفين أفراد عينـة الدراسـة بأسلوب واضح ومبسط قبل توزيع الاستبانة، كما وقام بشرح طريقة الإجابة، مع عدم ترك فقرة بدون إجابة وعدم وضع أكثر من إجابة للفقرة الواحدة.

وبعد أن قام الباحث بالرد على استفسارات بعض الموظفين، قام بتوزيع الاستبانة علـيهم حيث بلغت عينة الدراسة (58).

3- زمن تطبيق الاستبانة:

عند تطبيق الأداة استطلاعيا تبين ان الزمن المناسب لانتهاء المفحوص من الإجابة على الفقرات هي حوالي(25) دقيقة.

المعالجة الإحصائية :

لتحقيق أهداف الدراسة تم استخدام المعالجات الإحصائية التالية:

1- المتوسط الحسابي والانحراف المعياري.

2- التكرارات والنسب المئوية.

3- اختبار التحليل التباين الأحادي

4- ترتيب الفقرات ومستوى الدلالة

5- درجات الحرية

وقد تمت المعالجات الإحصائية باستخدام برنامج SPSS.

الفصل الخامس

تحليل وتفسير فقرات الدراسة

واختبار الفرضيات

لقد تم تصميم فقرات الإستبانة لتبين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات للوصول إلى أفضل النتائج، وفيما يلي عرض لنتائج الدراسة:

أولاً: الإجابة على الأسئلة المغلقة :

تم إدراج تسعة أسئلة مغلقةً للإحاطة بمدى اهتمام العاملين في مراكز تكنولوجيا المعلومات باستخدام التوقيع الإلكتروني، والجداول التالية تلخص نتائج تلك الأسئلة وكانت على النحو التالي:

هل سبق وأن استخدمت التوقيع الإلكتروني؟

جدول رقم (5.1)

مدى استخدام التوقيع الإلكتروني من قبل موظفي مراكز تكنولوجيا المعلومات

الإجابة	العدد	النسبة المئوية
نعم	16	27.59
لا	42	72.41
المجموع	**58**	**100**

من الجدول رقم (5.1) يتبين أن 27.59% فقط من نسبة أفراد العينة سبق لهم وان استخدموا التوقيع الإلكتروني، حيث أن هؤلاء الموظفين قد استخدموا التوقيع الإلكتروني بشكل فردي في مراسلاتهم الخاصة بينما لم يتم استخدامه بشكل رسمي في مراكز تكنولوجيا المعلومات. و هذا ما يبرر ارتفاع نسبة الإجابة بـ "لا" .

ما هي الفترة الزمنية للذين سبق وأن استخدموا التوقيع الإلكتروني؟

الجدول رقم (5.2)

يوضح النسبة المئوية للفترة الزمنية للذين سبق وأن استخدموا التوقيع الإلكتروني

الفترة الزمنية	العدد	النسبة المئوية
أقل من سنة	4	6.90
من سنة - سنتين	8	13.79
من 2-5 سنوات	3	5.17
أكثر من 5 سنوات	1	1.72
المجموع	**16**	**27.59**

يتضح من الجدول (5.2) أن أعلى نسبة للفترة الزمنية لاستخدام التوقيع الإلكتروني كانت مقابل فئة من (سنة- سنتين)، ويعزو الباحث ذلك إلى انخفاض عدد سنوات الخبرة لدى موظفي مراكز تكنولوجيا المعلومات في مجال عملهم وهذا يتوافق مع نتيجة الجدول رقم (4.6) من الفصل الرابع.

3- هل المؤسسات التعليمية بحاجة إلى استصدار تشريع من المجلس التشريعي للسماح باستخدام التوقيع الإلكتروني فيما بينهم وبين المؤسسات الأخرى؟

الجدول رقم (5.3)

مدى الحاجة لإصدار تشريع من المجلس التشريعي لإستخدام التوقيع الإلكتروني بين المؤسسات

الإجابة	العدد	النسبة المئوية
نعم	43	74.14
لا	15	25.86
المجموع	**58**	**100.00**

يتضح من الجدول رقم (5.3) أن 74.14% يؤيدون استصدار تشريع من المجلس التشريعي للسماح باستخدام التوقيع الإلكتروني فيما بين المؤسسات ويعزو الباحث هذة النتيجة الجيدة إلى أن التوقيع الإلكتروني بحاجة إلى تشريع لحماية العقود الإلكترونية المبرمة بين المؤسسات كما في العقود التقليدية بينما في حالة الإجابة بـ "لا" أن نتيجة لعدم استخدامهم التوقيع الإلكتروني مسبقاً وهذا يتوافق مع نتيجة الجدول رقم (5.1).

4- هل هناك توجه لإستخدام التوقيع الإلكتروني في مركز تكنولوجيا المعلومات؟

الجدول رقم (5.4)

مدى التوجه لإستخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات

الإجابة	العدد	النسبة المئوية
نعم	28	48.28
لا	30	51.72
المجموع	**58**	**100.00**

بالنظر إلى الجدول رقم (5.4) يتبين ان 51.72% يعتقدون انه لا يوجد توجه لدى إدارة مراكز تكنولوجيا المعلومات لاستخدام التوقيع الإلكتروني ويعزو الباحث ذلك إلى ضعف الكفاءات الموجودة حالياً في هذة المراكز وكذلك إلى وجود قصور مادي لدي مراكز تكنولوجيا المعلومات.

5- هل سبق وأن تم إختراق أنظمة الحاسوب في الجامعة ؟

الجدول رقم (5.5)

مدى إختراق أنظمة الحاسوب في الجامعة

الإجابة	العدد	النسبة المئوية
نعم	19	32.76
لا	17	29.31
ليس ضمن مجال عملي	22	37.93
المجموع	**58**	**100.00**

يتضح من الجدول رقم (5.5) ان 32.76% يعتقدون انه تم اختراق أنظمة الحاسوب في الجامعة وذلك نتيجة لعدم توفر الامكانيات المادية لحماية أمن المعلومات، وأن أنظمة الحماية المستخدمة بحاجة إلى تحديث وهذا يتناسب مع نتيجة الفقرة (1) و(2) من الجدول رقم (5.6) حسب الترتيب.

6- ما أسباب اختراق أنظمة المعلومات في الجامعات الفلسطينية

الجدول رقم (5.6)

أسباب اختراق أنظمة المعلومات في الجامعات الفلسطينية

#	الأسباب	العدد	النسبة المئوية	الترتيب
1	عدم توفر الامكانيات المادية لحماية أمن المعلومات	10	17.24	1
2	أنظمة الحماية المستخدمة بحاجة إلى تحديث	8	13.79	2
3	ضعف الخبرات التقنية لموظفي المركز	7	12.07	3
4	عدم توفر المعدات والبرمجيات الخاصة بحماية أمن المعلومات	6	10.34	4
5	أمن المعلومات ليس من اهتمام الإدارة العليا لمركز تكنولوجياالمعلومات	4	6.90	5

يتضح من الجدول رقم (5.5) أن أكثر الأسباب لاختراق أنظمة المعلومات في الجامعـات الفلسطينية هو " **عدم توفر الامكانيات المادية لحماية أمن المعلومات**" حيث حصل علـى المرتبـة الأولى من الأسباب، تلى ذلك " **أنظمة الحماية المستخدمة بحاجة إلى تحديث**" حيث حـصل علـى المرتبة الثانية من أسباب الإختراق، تلى ذلك" **ضعف الخبرات التقنية لموظفي المركز**" حيث حصل على المرتبة الثالثة من الأسباب، تلى ذلك " **عدم توفر المعدات والبرمجيات الخاصة بحماية أمـن المعلومات**" حيث حصل على المرتبة الرابعة، تلى ذلك " **أمن المعلومات ليس من اهتمـام الإدارة العليا لمركز الحاسوب**" حيث حصل على المرتبة الأخيرة من أسباب اختراق أنظمة المعلومات في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية.

7- هل هناك إجراءات دورية ومحددة يقوم بها مدير أمن المعلومات في المركز (أو من ينوب عنه) للحفاظ على أمن المعلومات؟

الجدول رقم (5.7)

وجود الإجراءات الدورية التي يقوم بها مدير أمن المعلومات في المركز

البيان	دائماً	غالباً	أحياناً	نادراً	مطلقاً	المتوسط	الانحراف المعياري	الوزن النسبي
الاستجابات	16	5	2	0	35	2.43	1.827	48.6
%	27.59	8.62	3.45	0	60.34			

يتبين من الجدول رقم (5.7) أن مدير أمن المعلومات أو من ينوب عنه للحفـاظ علـى أمن المعلومات لا يقومون بإجراءات دورية للحفاظ على أمن المعلومات وهذا ما تؤكده الإجابـة بـ " مطلقاً" حيث بلغت النسبة المئوية 60.34% ، ويعزو الباحث ذلك لعدم وجـود موظـف بمسمى "مدير أمن المعلومات في مراكز تكنولوجيا المعلومات" (حسب المسمى الوظيفي للفقـرة رقم (7) في الإستبانة التي قام الباحث بتوزيعها) أو دائرة متخصصة في حماية أمن المعلومـات للقيام باجراءات دورية ومحددة للحفاظ على أمن المعلومات الإلكترونية، وأن الـوزن النـسبي لوجود الإجراءات هو 48.6% وهو وزن ضعيف أقل من 50%، وهذا يعني أن عينة الدراسة يعتقدون أن الإجراءات الدورية ضعيفة.

8- هل إدارة مركز تكنولوجيا المعلومات تتبع معايير محددة خاصة بأمن المعلومات يتم تحديثها بشكل مستمر؟

الجدول رقم (5.8)

مدى اتباع وتحديث المعايير الخاصة بأمن المعلومات من قبل إدارة المركز

الإجابة	العدد	النسبة المئوية
نعم	16	27.59
لا	42	72.41
المجموع	**58**	**100.00**

الجدول رقم (5.8) يبين أن 72.41% من المستبانين يعتقدون ان إدارة مراكز تكنولوجيا المعلومات لا تتبع معايير محددة خاصة بأمن المعلومات يتم تحديثها بشكل مستمر ويعزو الباحث ذلك إلى عدم وجود موظف بمسمى وظيفي" مدير أمن المعلومات" في مراكز تكنولوجيا المعلومات (حسب المسمى الوظيفي للفقرة رقم (7) من الإستبانة) لتطبيق المعايير الخاصة بأمن المعلومات وتحديثها باستمرار.

9- هل برمجيات أمن المعلومات المستخدمة حالياً في المركز من إنتاج قسم البرمجة في المركز؟

الجدول رقم (5.9)

مدى إنتاج قسم البرمجة لبرمجيات أمن المعلومات المستخدمة حالياً في المركز

البيان	جميعها	بعضها	لا يوجد	المتوسط	الانحراف المعياري	الوزن النسبي
الاستجابات	18	24	16	2.03	0.772	67.66
%	31.03	41.38	27.59			

بالنظر إلى الجدول رقم (5.9) يتضح أن 31.03% يعتقدون أن جميع برمجيات أمن المعلومات من إنتاج قسم البرمجة، وأن 41.38% يعتقدون ان بعض برمجيات آمن المعلومات المستخدمة حالياً في المركز هى من إنتاج قسم البرمجة في المركز، بينما يرى 27.59% من أفراد العينة أن قسم البرمجة لا ينتج برمجيات لأمن المعلومات، وبالنظر إلى الوزن النسبي نجد أنه 67.66% وهي نسبة مقبولة ولا نستطيع أن نقول كبيرة، ويعزو الباحث تدني هذة النسبة من ان المقصود ببعض البرمجيات هو قيام المبرمجين في قسم البرمجة بتفعيل وعمل إعدادات

أمنية متوفرة ضمن قواعد البيانات المعتمدة في المركز مثل قواعد بيانات (oracle) ولا يقصد بها إنشاء برامج أمنية مستقلة لحماية بيانات المركز من الإختراق، بالإضافة إلى عدم الإطـلاع الكافي على تطورات برمجيات أمن المعلومات من قبل موظفي قـسم البرمجـة فـي مراكـز تكنولوجيا المعلومات في الجامعات الفلسطينية وهذا يتوافق مع نتيجة الجدول رقـم (5.4) فـي سلبية التوجة لإستخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات ممـا سـيؤدي إلـى ظهور فجوة بين التطورات التقنية الحديثة في مجال أمن المعلومات وتدني خبرات موظفي قسم البرمجة مع مرورالوقت.

ثانياً : تحليل فقرات مجالات الدراسة

1. تحليل فقرات المجال الأول والمتعلقة بـ " تطـوير البنيـة التحتيـة لمراكـز تكنولوجيـا المعلومات".

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5.10)، والذي يبين أن الوزن النسبي لجميع فقرات المجال أكبر من الوزن النسبي المحايد "60%" حيث تراوح الـوزن النسبي بين 61.38 % و 71.72% وكذلك بلغت قيمة مستوى الدلالة المعنوية لكل فقرة أقل من 0.05.

جدول (5.10)

ترتيب كل فقرة من الفقرات المتعلقة بتطوير البنية التحتية لمراكز تكنولوجيا المعلومات تبعاً للمتوسطات الحسابية والوزن النسبي ومستوى الدلالة والترتيب (ن = 58)

م	السؤال	المتوسط الحسابي	الوزن النسبي	قيمة t	مستوى الدلالة	الترتيب
1	يستخدم مركز تكنولوجيا المعلومات تقنيات بديلة عن التوقيع الإلكتروني؟	3.29	65.86	2.106	0.040	5
2	موازنة مركز تكنولوجيا المعلومات تسمح بإنشاء بنية تحتية لتقنية التوقيع الإلكتروني	3.22	64.48	1.691	0.096	6
3	يدرك موظفو مركز تكنولوجيا المعلومات بأهمية استخدام التوقيع الإلكتروني	3.59	71.72	4.147	0.000	1
4	المعدات الأمنية المستخدمة في مركز تكنولوجيا المعلومات لحماية المراسلات الإلكترونية تواكب التطور التقني	3.52	70.34	4.271	0.000	2
5	البرمجيات الأمنية المستخدمة في مركز تكنولوجيا المعلومات لحماية المراسلات الإلكترونية يتم تحديثها بشكل مستمر	3.48	69.66	3.512	0.001	3
6	موظفو مركز تكنولوجيا المعلومات على إطلاع مستمر بتطور تقنيات أمن المعلومات بشكل عام وبتقنية التوقيع الإلكتروني بشكل خاص	3.07	61.38	0.475	0.637	7
7	موظفو مركز تكنولوجيا المعلومات يمتلكون مؤهلات وخبرات تقنية جيدة في إنشاء تقنيات أمن المعلومات وخاصة تقنية التوقيع الإلكتروني	3.48	69.66	3.630	0.001	4
	جميع فقرات المجال الأول	**23.66**	**67.59**	**4.592**	**0.000**	

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.05) = 2.00

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.01) = 2.66

يتضح من الجدول رقم (5.10)، أن الفقرة رقم (3) احتلت المرتبة **الأولى** والمتعلقة بـ "يدرك موظفو مركز تكنولوجيا المعلومات بأهمية استخدام التوقيع الإلكتروني" حيث بلغ الـوزن النسبي لتلك الفقرة 71.72% ويعزو الباحث تلك النتيجة الجيدة إلى بدأ إدراك موظفي مراكـز تكنولوجيا المعلومات بأهمية أمن المعلومات وحماية المراسلات الإلكترونية.

الفقرة رقم (4) احتلت المرتبة **الثانية** والمتعلقة بـ "المعدات الأمنيـة المـستخدمة فـي مركز تكنولوجيا المعلومات لحماية المراسلات الإلكترونية تواكب التطور التقنـي" حيـث بلـغ الوزن النسبي لتلك الفقرة 70.34% وهذة النتيجة تدل على أن المعدات الأمنية المتـوفرة فـي مراكز تكنولوجيا المعلومات معدات قادرة على حماية البيانات الإلكترونية إلى حـدٍ مـا لكنهـا بحاجة إلى تحديث لتواكب المعدات العالمية المتطورة.

وبالنظر إلى الفقرة رقم (5) احتلت المرتبة **الثالثة** والمتعلقة بـ " البرمجيـات الأمنيـة المستخدمة في مركز تكنولوجيا المعلومات لحماية المراسلات الإلكترونية يتم تحـديثها بـشكل مستمر" ، وبوزن نسبي قدره 69.66% وهذة النتيجة تدل على ان البرمجيات المستخدمة فـي مراكز تكنولوجيا المعلومات بحاجة إلى تطوير لتواكب تطورات البرمجيـات الأمنيـة الحديثـة لتكون قادرة على حماية المعلومات الحساسة في مراكز تكنولوجيا المعلومات.

الفقرة رقم (7) كانت في المرتبة **الرابعة** والمتعلقة بـ " موظفـو مركـز تكنولوجيـا المعلومات يمتلكون مؤهلات وخبرات تقنية جيدة في إنشاء تقنيات أمن المعلومات وخاصة تقنية التوقيع الإلكتروني"، حيث بلغ الوزن النسبي لتلك الفقرة 69.66% ويعزو الباحث ذلك إلـى أن موظفي مراكز تكنولوجيا المعلومات يمتلكون الأساسيات لإنشاء تقنيات أمن المعلومـات لكـنهم بحاجة إلى المزيد من التدريب والتطوير والإطلاع علـى تقنيـات أمـن المعلومـات لمواكبـة التطورات التقنية في مجال أمن المعلومات وهذا يتوافق نتيجة الفقرة رقم (6).

واحتلت الفقرة رقم (1) المرتبة **الخامسة** والمتعلقة بـ " يـستخدم مركـز تكنولوجيـا المعلومات تقنيات بديلة عن التوقيع الإلكتروني"، حيث بلغ الوزن النسبي لتلـك الفقـرة 65.86 ويعزو الباحث ذلك إلى وجود قصور لدى موظفي مراكز تكنولوجيا المعلومات لمفهوم التوقيـع الإلكتروني واستخدامه وإلى ضعف اطلاع موظفي المراكـز علـى تطـورات تقنيـات أمـن المعلومات وهذا يتناسب مع نتيجة الفقرة رقم (6).

من الملاحظ ان الفقرة رقم (2) احتلت المرتبة **السادسة** والمتعلقة بـ " موازنة مركـز تكنولوجيا المعلومات تسمح بإنشاء بنية تحتية لتقنية التوقيع الإلكتروني" ، حيـث بلـغ الـوزن النسبي لتلك الفقرة 64.48% ويعزو الباحث ذلك إلـى ان الإدارة العليـا لمراكـز تكنولوجيـا

المعلومات لا تعمل ضمن خطة استراتيجة واضحة وهذا يتوافق مع نتيجة الفقرة (15)، كذلك لا تعمل على تحديث وإنشاء تقنيات خاصة بأمن المعلومات وهذا يتناسب مع نتـائج الفقـرات (8) و(9).

بالنظر إلى الجدول رقم (5.10) نلاحظ أن الفقرة رقم (6) احتلت المرتبة **الـسابعة** – الأخيرة- والمتعلقة بـ " موظفو مركز تكنولوجيا المعلومات على إطلاع مستمر بتطور تقنيـات أمن المعلومات بشكل عام وبتقنية التوقيع الإلكتروني بشكل خـاص" ، وبـوزن نـسبي قـدره 61.38% ويعزو الباحث تدني هذة النسبة إلى أن موظفي مراكز تكنولوجيا المعلومات لـديهم قصور في متابعة تطورات تكنولوجيا أمن المعلومات وهذا يتنافى وطبيعة عملهـم فـي مجـال تكنولوجيا المعلومات.

وبصفة عامة بلغ المتوسط الحسابي لجميع فقـرات المجـال الأول 23.66 والـوزن النسبي 67.59 % ومستوى المعنوية 0.000 وهو اقل من 0.05 مما يدل على وجود بنيـة التحتية لأمن المعلومات في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية لكنها بحاجة إلى تحديث لتواكب التطورات التقنية الحديثة في مجال أمن المعلومات مـن حيـث التقنيـات والمعدات والبرمجيات المستخدمة والموارد البشرية.

- إيجاد معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيـا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين تطوير البنية التحتية لهذة المراكـز، وللتحقق من ذلك تم استخدام معامل ارتباط بيرسون والجدول رقم (5.11) يوضح ذلك:

جدول رقم (5.11)

يوضح معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين تطوير البنية التحتية لهذة المراكز

المجال	المجموع
تطوير البنية التحتية لمراكز تكنولوجيا المعلومات	**0.821

* قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.05) = 0.250

** قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.01) = 0.325

يتضح من الجدول رقم (5.11) وجود علاقة ارتباطية موجبة ذات دلالة إحصائية عنـد مستوى دلالة 0.01 بين متطلبات استخدام التوقيع الالكترونـي فـي إدارة مراكـز تكنولوجيـا

المعلومات في الجامعات الفلسطينية في قطاع غزة وبين تطوير البنية التحتية لهذة المراكـز، أي أن البنية التحتية لمراكز تكنولوجيا المعلومات تعتبر من متطلبات استخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية مما يعني قبول الفرضية.

ويعزو الباحث ذلك الى ان توفير البنية التحتية المتطـورة لـدى مراكـز تكنولوجيـا المعلومات واستخدامها بالشكل الأمثل يؤدي إلى قدرة هذة المراكز على استخدام تقنيات متطورة في مجال امن المعلومات ومنها تقنية التوقيع الإلكتروني لتواكب التطورات التقنية الحديثة لحماية المعلومات الإلكترونية في هذة المراكز.

وبذلك يتبين وجود علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعـات الفلسطينية في قطاع غزة وبين تطوير البنية التحتية لمراكز تكنولوجيا المعلومات.

2. تحليل فقرات المجال الثاني والمتعلق بـ " "اهتمـام الإدارة العليـا لمراكـز تكنولوجيـا المعلومات باستخدام التوقيع الالكتروني"

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5.12)، والذي يبين أن الوزن النسبي لجميع فقرات المجال أكبر من الوزن النسبي المحايد "60%" حيث تراوح الـوزن النسبي بين 53.10 % و 74.83% وكذلك بلغت قيمة مستوى الدلالة لكل فقرة أقل من 0.05، والجدول رقم (5.12) يوضح ذلك :

جدول (5.12)

ترتيب كل فقرة من الفقرات المتعلقة باهتمام الإدارة العليا لمراكز تكنولوجيا المعلومات باستخدام التوقيع الالكتروني تبعاً للمتوسطات الحسابية والوزن النسبي ومستوى الدلالة والترتيب (ن = 58)

م	السؤال	المتوسط الحسابي	الوزن النسبي	قيمة t	مستوى الدلالة	الترتيب
8	استخدام تقنية التوقيع الإلكتروني مدرجة ضمن الخطة الإلستراتيجية لمركز تكنولوجيا المعلومات	3.21	64.14	1.493	0.141	7
9	تعمل إدارة مركز تكنولوجيا المعلومات على إنشاء البنية التحتية لتقنية التوقيع الإلكتروني	3.05	61.03	0.394	0.695	8
10	إدارة مركز تكنولوجيا المعلومات على اطلاع مستمر بالتطورات التقنية لأمن المعلومات	3.55	71.03	4.018	0.000	2
11	إدارة مركز تكنولوجيا المعلومات على إطلاع بأهمية استخدام التوقيع الإلكتروني	3.40	67.93	2.899	0.005	4
12	إدارة مركز تكنولوجيا المعلومات حريصة على تطوير موظفي المركز بصورة مستمرة في مجال آمن المعلومات	3.28	65.52	1.622	0.110	5
13	تعتمد إدارة مركز تكنولوجيا المعلومات المراسلات الإلكترونية	3.74	74.83	5.203	0.000	1
14	تعتمد إدارة مركز تكنولوجيا المعلومات الشهادات الرقمية للخادم الرئيسي في المركز وللمراسلات الإلكترونية	2.66	53.10	-2.829	0.006	9
15	تعمل إدارة مركز تكنولوجيا المعلومات ضمن خطة إستراتيجية واضحة	3.22	64.48	1.585	0.118	6
16	إدارة مركز تكنولوجيا المعلومات قادرة على إدارة المركز بكفاءة	3.52	70.34	3.762	0.000	3
	جميع فقرات المجال الثاني	**29.62**	**65.82**	**3.141**	**0.003**	

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.05) = 2.00

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.01) = 2.66

يتبين من الجدول رقم (5.12)، أن الفقرة رقم (13) احتلت المرتبة **الأولى** والمتعلقة بـ "تعتمد إدارة مركز تكنولوجيا المعلومات المراسلات الإلكترونية"، وبوزن نسبي قدره 74.83%، ويعزو الباحث هذة النتيجة الجيدة إلى أهمية استخدام المراسلات الإلكترونية في إدارة مراكز تكنولوجيا المعلومات مما توفره من وقت وجهد وزيادة سرعة المراسلات الإلكترونية وسهولة الأرشفة وهذا يتناسب مع هدف ومفهوم تكنولوجيا المعلومات .

كما يلاحظ أن الفقرة رقم (10) احتلت المرتبة **الثانية** والمتعلقة بـ " إدارة مركز تكنولوجيا المعلومات على اطلاع مستمر بالتطورات التقنية لأمن المعلومات"، حيث بلغ الوزن النسبي لتلك الفقرة 71.03% وهذا يبين إدراك الإدارات العليا لمراكز تكنولوجيا المعلومات بأهمية حماية البيانات الإلكترونية.

وبالنظر إلى الجدول رقم (5.12) نلاحظ أن الفقرة رقم (16) احتلت المرتبة **الثالثة** والمتعلقة بـ "إدارة مركز تكنولوجيا المعلومات قادرة على إدارة المركز بكفاءة "، حيث بلغ الوزن النسبي لتلك الفقرة 70.34% ويعزو الباحث ذلك أن إدارات مراكز تكنولوجيا المعلومات تقوم بإدارة المراكز بكفاءة ولكن من خلال عمل الباحث في مراكز تكنولوجيا المعلومات ومن خلال المقابلات الشخصية تبين للباحث وجود بعض المواقع في الإدارات العليا لمراكز تكنولوجيا المعلومات من غير المتخصصين في مجال تكنولوجيا المعلومات.

واحتلت الفقرة رقم (11) المرتبة **الرابعة** والمتعلقة بـ " إدارة مركز تكنولوجيا المعلومات على إطلاع بأهمية استخدام التوقيع الإلكتروني"، وبوزن نسبي قدره 67.93%، ويعزو الباحث أن إدارة مراكز تكنولوجيا المعلومات تدرك أهمية استخدام التوقيع الإلكتروني وهذا يتوافق مع الفقرة رقم (10)، لكن الباحث يعتبر ان هذة النسبة تعتبر متدنية نظراً لأهمية أمن المعلومات وحساسيتها وسرية المعاملات الإلكترونية في مراكز تكنولوجيا المعلومات لهذا كان من الأفضل أن تكون النسبة في درجة متقدمة نظراً لأهمية التوقيع الإلكتروني في المحافظة على أمن المعلومات.

كما احتلت الفقرة رقم (12) المرتبة **الخامسة** والمتعلقة بـ "إدارة مركز تكنولوجيا المعلومات حريصة على تطوير موظفي المركز بصورة مستمرة في مجال آمن المعلومات" حيث بلغ الوزن النسبي لتلك الفقرة 65.52%، ويعزو الباحث ذلك إلى قصور في الخطط التدريبية وتطبيقها لتطوير موظفي مراكز تكنولوجيا المعلومات بشكل مستمر في مجال أمن المعلومات لمواكبة التطور التقني المتسارع في مجال أمن المعلومات وهذا يتوافق مع نتيجة الفقرات رقم (6) و (7)، وإلا سيؤدي إلى ظهور فجوة تقنية تزداد مع مرور الوقت في عدم إدراك مفهوم التقنيات المتطورة وهذا يتوافق مع نتيجة الفقرة رقم (1).

ويتبين أن الفقرة رقم (15) احتلت المرتبة **السادسة** والمتعلقة بـ " تعمل إدارة مركز تكنولوجيا المعلومات ضمن خطة إستراتيجية واضحة"، وبوزن نسبي 64.48%، ويعزو الباحث ذلك إلى أن الخطط الإستراتيجية لمراكز تكنولوجيا المعلومات غير واضحة وغير موضوعة بناء على دراسات معمقة وهذا يدل إلى عدم وضوح الرؤية المستقبلية للإدارة العليا لمراكز تكنولوجيا المعلومات.

كما احتلت الفقرة رقم (8) المرتبة **السابعة** والمتعلقة بـ " استخدام تقنية التوقيع الإلكتروني مدرجة ضمن الخطة الإستراتيجية لمركز تكنولوجيا المعلومات"، حيث بلغ الوزن النسبي لتلك الفقرة 64.14% ويعزو الباحث ذلك إلى أن مضمون الخطة الإستراتيجية لمراكز تكنولوجيا المعلومات غير واضحة وهذا ما تؤكده الفقرة (15).

وبالنظر إلى الجدول رقم (12) كذلك فإن الفقرة رقم (9) احتلت المرتبة **الثامنة** والمتعلقة بـ " تعمل إدارة مركز تكنولوجيا المعلوماتعلى إنشاء البنية التحتية لتقنية التوقيع الإلكتروني "، حيث بلغ الوزن النسبي لتلك الفقرة 61.03% ويعزو الباحث تدني النسبة إلى عدم وضوح الخطة الإستراتيجية الخاصة بمراكز تكنولوجيا المعلومات وضبابية المحتوى وهذا يتوافق مع الفقرات (8) و(15).

من الملاحظ ان الفقرة رقم (14) احتلت المرتبة **التاسعة – الأخيرة-** والمتعلقة بـ" تعتمد إدارة مركز تكنولوجيا المعلومات الشهادات الرقمية للخادم الرئيسي في المركز وللمراسلات الإلكترونية "، حيث بلغ الوزن النسبي لتلك الفقرة 53.10%، ويعزو الباحث سلبية الإجابة إلى أن مراكز تكنولوجيا المعلومات لا تستخدم الشهادات الرقمية Digital Certificates في الخادم الرئيس أو للمراسلات الإلكترونية وهذا يتوافق مع نتائج الفقرة (24) من المجال الرابع.

من الجدول رقم (5.12) يتبين أن المتوسط الحسابي لجميع فقرات المجال الثاني بلغ 29.62 والوزن النسبي 65.82 % ومستوى الدلالة 0.003 وهو اقل من 0.05 مما يدل على ان الإدارة العليا لمراكز تكنولوجيا المعلومات لديها اهتمام باستخدام التوقيع الالكتروني.

- إيجاد معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني، وللتحقق من ذلك تم استخدام معامل ارتباط بيرسون والجدول رقم (5.13) يوضح ذلك:

جدول (5.13)

يوضح معامل الارتباط بين واقع استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني.

المجال	المجموع
اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني	0.885**

* قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.05) = 0.250

** قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.01) = 0.325

يتضح من الجدول رقم (5.13) وجود علاقة ارتباطية موجبة ذات دلالة إحصائية عند مستوى دلالة 0.01 بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني، أي أن اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني لمراكز تكنولوجيا المعلومات تعتبر من متطلبات استخدام التوقيع الإلكتروني في هذة المراكز مما يعني قبول الفرضية، ويعزو الباحث ذلك الى ان اهتمام الإدارة العليا لمراكز تكنولوجيا المعلومات باستخدام التوقيع الإلكتروني وأمن المعلومات يؤدي إلى استخدام تقنيات متطورة للحفاظ على أمن المراسلات الإلكترونية كتقنية التوقيع الإلكتروني.

وقد اتفقت نتيجة هذه الدراسة مع دراسة Thomas (2006) والتي توصلت إلى ان اهتمام الإدارة العليا له تأثير كبير على ثقافة الأمن وتطبيق السياسات الأمنية في المؤسسة، وكذلك فإن جميع برامج الأمن المتبعة في المؤسسة سوف تفشل رغم توفر التقنية المتطورة دون اهتمام حقيقي من الإدارة العليا لهذة البرامج ورعايتها.

وبذلك يتبين وجود علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني.

3. تحليل فقرات المجال الثالث والمتعلق بـ " وجود المتطلبات القانونية والتشريعية لاستخدام التوقيع الالكتروني"

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5.14)، والذي يبين أن الوزن النسبي لجميع فقرات المجال أكبر من الوزن النسبي المحايد "60%" حيث تراوح الوزن النسبي بين 66.21 % و 78.62% وكذلك بلغت قيمة مستوى المعنوية لكل فقرة أقل من 0.05، والجدول رقم (5.14) يوضح ذلك :

جدول (5.14)

ترتيب كل فقرة من الفقرات المتعلقة بوجود المتطلبات القانونية والتشريعية لاستخدام التوقيع الالكتروني تبعاً للمتوسطات الحسابية والوزن النسبي ومستوى الدلالة والترتيب (ن = 58)

م	السؤال	المتوسط الحسابي	الوزن النسبي	قيمة t	مستوى الدلالة	الترتيب
17	يلزم استصدار تشريع قانوني من المجلس التشريعي يسمح باستخدام التوقيع الإلكتروني بين دوائر الجامعة	3.31	66.21	1.856	0.069	5
18	استخدام التوقيع الإلكتروني بين أقسام ودوائر الجامعة بحاجة إلى موافقة الإدارة العليا للجامعة	3.93	78.62	7.304	0.000	1
19	يعتمد استخدام التوقيع الإلكتروني في المراسلات الإلكترونية بين أقسام مركز تكنولوجيا المعلوماتبأخذ موافقة إدارة المركز	3.41	68.28	2.972	0.004	4
20	التوقيع الإلكتروني بحاجة إلى استصدار قانون تشريعي من المجلس التشريعي لحمايته	3.93	78.62	7.046	0.000	2
21	إبرام العقود الإلكترونية يتم حمايتها قانونياً وتشريعياً	3.48	69.66	3.056	0.003	3
	جميع فقرات المجال الثالث	**18.07**	**72.28**	**5.870**	**0.000**	

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.05) = 2.00

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.01) = 2.66

الجدول رقم (5.14) يبين أن الفقرة رقم (18) احتلت المرتبة الأولى والمتعلقة بـ"استخدام التوقيع الإلكتروني بين أقسام ودوائر الجامعة بحاجة إلى موافقة الإدارة العليا للجامعة " ، وبوزن نسبي قدره 78.62 %، و يعزو الباحث هذة النتيجة الجيدة إلى ان استخدام تقنية التوقيع الإلكتروني بين أقسام ودوائر المؤسسة الواحدة – الجامعة- للحفاظ على أمن المعلومات للمؤسسة لا يحتاج إلى قانون تشريعي وإنما يحتاج إلى اعتماد الإدارة العليا للجامعة لأستخدام تقنيات متطورة لحماية المعلومات الداخلية لديها كتقنية التوقيع الإلكتروني، وهذة النتيجة تتوافق مع دراسة (Rodney, 2004) في أن على المؤسسات أن تقوم بالمحافظة وحماية المعلومات والبيانات الإلكترونية الداخلية لديها دون الحاجة لقانون أو تشريع لحمايتها.

كما احتلت الفقرة رقم (20) المرتبة الثانية والمتعلقة بـ " التوقيع الإلكتروني بحاجة إلى استصدار قانون تشريعي من المجلس التشريعي لحمايته "، وبوزن نسبي 78.62%، ويعزو الباحث هذة النسبة الجيدة إلى أن العقود الإلكترونية الموقعة بالتوقيع الإلكتروني بحاجة إلى حماية قانونية كما في العقود التقليدية لتطبيقها وحمايتها.

من الملاحظ أن الفقرة رقم (21) احتلت المرتبة الثالثة والمتعلقة بـ " إبـرام العقـود الإلكترونية يتم حمايتها قانونياً وتشريعياً "، وبوزن نسبي 69.66%، ويعزو الباحث ذلك إلى ان العقود الإلكترونية بحاجة إلى اصدار قانون تشريعي من المجلس التشريعي لحمايتها كمـا هـو الحال في العقود التقليدية.

بالنظر إلى الجدول رقم (5.14) يتبين أن الفقرة رقم (19) احتلـت المرتبـة الرابعـة والمتعلقة بـ " يعتمد استخدام التوقيع الإلكتروني في المراسلات الإلكترونية بين أقـسام مركـز تكنولوجيا المعلومات بأخذ موافقة إدارة المركز "، وبوزن نسبي 68.28%، ويعزو الباحث ذلك أن اعتماد التوقيع الإلكتروني في المراسلات الإلكترونية الرسمية بين أقسام مركـز تكنولوجيـا المعلومات يصدر وبمبادرة من الإدارة العليا للمركز وهذا يبين أن توجهـات وتـشجيع الإدارة العليا في استخدام التكنولوجيا المتطورة يؤدي إلى استخدامها من قبل بقية أقسام المركز.

واحتلت الفقرة رقم (17) المرتبة الخامسة والمتعلقة بـ " يلزم استصدار تشريع قانوني من المجلس التشريعي يسمح باستخدام التوقيع الإلكتروني بين دوائر الجامعة "، وبـوزن نـسبي 66.21%، ويعزو الباحث هذة النتيجة إلى عدم اطلاع موظفي مراكز تكنولوجيا المعلومـات حول القوانين المتعلقة باستخدام التوقيع الإلكتروني بشكل كافي، والتي تكون بحاجة لقانون فـي حالة إبرام العقود أو تبادل المراسلات الإلكترونية بين الجامعة والمؤسسات الخارجية الأخـرى لحمايتها وتنفيذها قانونياً، وهذا يتعارض مع الفقرات (18) و (19) وإنما يتوافق مع الفقرة (20) في حالة إبرام العقود الإلكترونية فيما بين المؤسسات.

وبصفة عامة بلغ المتوسط الحسابي لجميع فقرات المجـال الثالـث "وجـود المتطلبـات القانونية والتشريعية لاستخدام التوقيع الالكتروني" تساوي 18.07 والوزن النـسبي72.28 % ومستوى الدلالة 0.000 وهو أقل من 0.05 مما يدل على أن اسـتخدام التوقيـع الإلكترونـي بحاجة إلى وجود المتطلبات القانونية والتشريعية وهذا يعتبر أحد متطلبات اسـتخدام التوقيـع الإلكتروني.

ويعتقد الباحث أن التوقيع الإلكتروني يحتاج إلى وجود المتطلبات القانونيـة والتـشريعية لحمايته وذلك في حالة إبرام العقود الإلكترونية بين المؤسسات أو في حال تبـادل المراسـلات الإلكترونية بين الجامعة والمؤسسات الخارجية وهذا يتوافق مع نتيجة الفقرة رقم (20) حيث أن عدم وجود تشريع قانوني أدى إلى إحجام استخدام التوقيع الإلكتروني وهذا يتوافق مـع دراسـة

Borasky (1999)، حيث أن توفر المتطلبات القانونية يدعم التوجة لإستخدم التوقيع الإلكتروني مع مرور الوقت وهذا يتوافق أيضاً مع دراسة Edward (2004)، وهذا يتناقض مع دراسة Rodney (2004) في ان استخدام التوقيع الإلكتروني داخل المؤسسة لحماية المعلومات والمراسلات الإلكترونية لا يحتاج إلى قانون تشريعي لإعتماه داخل عمل المؤسسة، وإنما يحتاج إلى قرار من الإدارت العليا المختصة وهذا يتناسب مع نتائج الفقرات (18) و (19).

- إيجاد معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين **وجود المتطلبات القانونية والتشريعية لاستخدامه**، وللتحقق من ذلك تم استخدام معامل ارتباط بيرسون والجدول رقم (5.15) يوضح ذلك:

جدول (5.15)

يوضح معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين وجود المتطلبات القانونية والتشريعية.

المجال	المجموع
وجود المتطلبات القانونية والتشريعية لاستخدامه	0.625**

* قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.05) = 0.250

** قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.01) = 0.325

يتضح من الجدول رقم **(**5.15**)** وجود علاقة ارتباطية موجبة ذات دلالة إحصائية عند مستوى دلالة 0.01 بين واقع استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين وجود المتطلبات القانونية والتشريعية لاستخدامه، أي أن المتطلبات القانونية والتشريعية هي من متطلبات استخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات، مما يعني قبول الفرضية، ويعزو الباحث ذلك إلى أن استخدام التوقيع الإلكتروني في المراسلات الإلكترونية لمراكز تكنولوجيا المعلومات يحتاج إلى متطلبات قانونية خاصة في حال تبادل المراسلات وابرام العقود الإلكترونية بين مراكز تكنولوجيا المعلومات والمؤسسات الخارجية الاخرى بينما استخدام التوقيع الإلكتروني داخل الحرم الجامعي بين مركز تكنولوجيا المعلومات والدوائر الأخرى فإن ذلك يأتي من باب المحافظة على سرية وأمن المعلومات وحمايتها من حدوث أي تحريف أو كشف لهذة المعلومات من خلال شبكة الحاسوب

الداخلية حيث لا يحتاج إلى استصدار قانون تشريعي من المجلس التشريعي لحمايته وهذا يتوافق مع نتائج الفقرات (17) و (19)، ويتفق مع دراسة Rodney (2004) في أن استخدام التقنيات المتطورة لحماية معلومات المؤسسة الداخلية لا يحتاج إلى اصدار قانون لحماية هذه المعلومات.

وبذلك يتبين وجود علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين وجود المتطلبات القانونية والتشريعية لاستخدامه.

وبهذا يكون الباحث قد تحقق من عدم صحة الفرض الثالث من فروض الدراسة والذي نص على: لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين وجود المتطلبات القانونية والتشريعية لاستخدامه".

وبذلك يقبل بالفرض البديل، حيث تبين وجود علاقة بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين عدم وجود المتطلبات القانونية والتشريعية لاستخدامه.

4. تحليل فقرات المجال الرابع والمتعلق بـ " اعتماد المراسلات الالكترونية في مراكز تكنولوجيا المعلومات"

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5.16)، والذي يبين أن الوزن النسبي لجميع فقرات المجال أكبر من الوزن النسبي المحايد "60%" حيث تراوح الوزن النسبي بين 52.41 % و 76.21% وكذلك بلغت قيمة مستوى الدلالة لكل فقرة أقل من 0.05، والجدول رقم (5.16) يوضح ذلك :

جدول (5.16)

ترتيب كل فقرة من الفقرات المتعلقة بـ " اعتماد المراسلات الالكترونية في مراكز تكنولوجيا المعلومات" تبعاً للمتوسطات الحسابية والوزن النسبي ومستوى الدلالة والترتيب (ن = 58)

م	السؤال	المتوسط الحسابي	الوزن النسبي	قيمة t	مستوى الدلالة	الترتيب
22	يتم تبادل المراسلات الإلكترونية بين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعة إلكترونياً	3.52	70.34	3.236	0.002	4
23	يتم تبادل المراسلات إلكترونياً بين أقسام مركز تكنولوجيا المعلومات	3.81	76.21	5.457	0.000	1
24	تستخدم تقنية التوقيع الإلكتروني في المراسلات الإلكترونية لمركز تكنولوجيا المعلومات	2.62	52.41	-2.872	0.006	5
25	تتوفر الإمكانيات التقنية في مركز تكنولوجيا المعلومات لحفظ واعتماد المراسلات الإلكترونية	3.59	71.72	3.970	0.000	3
26	اعتماد المراسلات الإلكترونية بين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعة بحاجة إلى اعتماد الإدارة العليا للجامعة	3.64	72.76	4.169	0.000	2
	جميع فقرات المجال الرابع	**17.17**	**68.69**	**4.065**	**0.000**	

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.05) = 2.00

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.01) = 2.66

يتبين من الجدول رقم **(**5.16**)**، أن الفقرة رقم (23) احتلت المرتبة **الأولى** والمتعلقة بـ " يتم تبادل المراسلات إلكترونياً بين أقسام مركز تكنولوجيـا المعلومـات"، و وبـوزن نـسبي 76.21**%**، ويعزو الباحث ذلك إلى تبادل استخدام المراسلات الإلكترونية بشكل كبير وضـعف تبادل المراسلات الورقية بين أقسام مراكز تكنولوجيا المعلومات.

واحتلت الفقرة رقم (26) المرتبة **الثانية** والمتعلقة بـ " اعتماد المراسلات الإلكترونيـة بين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعة بحاجة إلى اعتماد الإدارة العليـا للجامعة " ، وبوزن نسبي 72.76%، ويعزو الباحث أن اعتماد المراسـلات إلالكترونيـة بـين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعة يحتـاج إلـى موافقـة الإدارة العليـا للجامعة وهذا ينسجم مع الفقرة (18) في المجال الثالث.

ويلاحظ أن الفقرة رقم (25) احتلت المرتبة **الثالثة** والمتعلقة بـ " تتـوفر الإمكانيـات التقنية في مركز تكنولوجيا المعلومات لحفظ واعتماد المراسلات الإلكترونية "، حيث بلغ الوزن

النسبي 71.72%، ويعزو الباحث ذلك إلى توفر البنية التحتية في مراكز تكنولوجيا المعلومـات لحفظ واعتماد المراسلات الإلكترونية وهذا ينسجم مع الفقرات (18) و (19) من المجال الأول.

وبالنظر إلى الجدول رقم (5.16) نلاحظ أن الفقرة رقم (22) احتلت المرتبة **الرابعـة** والمتعلقة بـ " يتم تبادل المراسلات بين مركز تكنولوجيا المعلومات والـدوائر الأخـرى فـي الجامعة إلكترونياً "، وبوزن نسبي 70.34%، ويعزو الباحث ذلك إلى أن مراكـز تكنولوجيـا المعلومات تستخدم المراسلات الإلكترونية بشكل كبير بينها وبين دوائر الجامعة الأخرى وهـذا يتوافق مع الفقرة (28).

من الملاحظ أن الفقرة رقم (24) احتلت المرتبة **الخامسة** – الأخيرة- والمتعلقة بـ " تُستخدم تقنية التوقيع الإلكتروني في المراسلات الإلكترونية لمركـز تكنولوجيـا المعلومـات"، وبوزن نسبي 52.41%، ويعزو الباحث سلبية الإجابة إلى أن مراكز تكنولوجيا المعلومـات لا تستخدم تقنية التوقيع الإلكتروني.

من الجدول رقم (5.16) يتبين أن المتوسط الحسابي لجميع فقرات المجال الثاني بلـغ 17.17 والوزن النسبي 68.69% ومستوى الدلالة 0.000 وهو اقل من 0.05 مما يدل على ان مراكز تكنولوجيا المعلومات تعتمد المراسلات الالكترونية.

ويعزو الباحث ذلك إلى أن استخدام المراسلات الإلكترونية يعمل على انجاز المعاملات بشكل أسرع وأكثر أمناً وتوفيراً للوقت والجهد والتكلفة مقارنة باستخدام المعاملات والمراسلات الورقة وهذا يتوافق مع دراسة Christopher (2007) في أن اسـتخدام التوقيـع الإلكترونـي يجعل المعاملات الإلكترونية أكثر أمناً وتبني الأنظمة الملائمة لتقنية التوقيع الإلكتروني تقلل في التكاليف، وهذا يتوافق كذلك مع دراسة Wilson (1998) ، في ان الكثير من العمـل سـينجز إلكترونياً دون استخدام المعاملات الورقية.

- إيجاد معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيـا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اعتمـاد المراسـلات الإلكترونيـة، وللتحقق من ذلك تم استخدام معامل ارتباط بيرسون والجدول رقم (5.17) يوضح ذلك:

جدول (5.17)

يوضح معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اعتماد المراسلات الإلكترونية.

المجال	المجموع
اعتماد المراسلات الإلكترونية	0.763**

* قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.05) = 0.250

** قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.01) = 0.325

يتضح من الجدول رقم (5.17) إلى وجود علاقة ارتباطية موجبة ذات دلالة إحـصائية عند مستوى دلالة 0.01 بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيـا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اعتماد المراسلات الإلكترونية مما يعني قبول الفرضية أي ان استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومـات فـي الجامعات الفلسطينية في قطاع غزة يزداد باعتماد المراسلات الإلكترونية وهذا ينسجم مع طبيعة عمل هذة المراكز.

ويعزو الباحث ذلك إلى أن مراكز تكنولوجيا المعلومات تعتمد المراسلات الإلكترونيـة في علاقتها الإدارية مع دوائر وأقسام الجامعة الأخرى لما تتميز به المراسلات الإلكترونية مـن التكاملية والسرية وتوفير الوقت والتكاليف حيث تتنوع المراسلات الإلكترونية إلى (ملف نصي، ملف رسومات، ملف وسائط متعددة أو ....إلخ) وبالتالي زيادة قيمة المعلومات داخل المؤسـسة مما يتيح إلى توفر مصادر معلومات متنوعة داخل المؤسسة وهذا يحتـاج إلـى حمايـة هـذة المراسلات الإلكترونية أثناء تنقلها عبر شبكة الحاسوب مما يستدعي الحاجة إلى استخدام التوقيع الإلكتروني في المراسلات الإلكترونية لحمايتها حيث تبـين الدراسـة مـدى كفـاءة اسـتخدام المراسلات الإلكترونية مقارنة بالمراسلات الورقية وهذا يتوافق مع دراسة David (2001).

وبذلك يكون الباحث قد تحقق من عدم صحة الفرض الرابع من فروض الدراسة والذي نص على: "لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيـا المعلومـات فـي الجامعـات الفلسطينية في قطاع غزة وبين اعتماد المراسلات الإلكترونية "

وعليه يقبل الباحث بالفرض البديل، حيث تبين وجود علاقة ارتباطية ذات دلالة إحصائية عنـد مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيـع الإلكترونـي فـي إدارة مراكـز

تكنولوجيا المعلومات في الجامعات الفلسطينية في قطـاع غـزة وبـين اعتمـاد المراسـلات الإلكترونية .

5. تحليل فقرات المجال الخامس والمتعلق بـ " سياسات حماية المعلومات الإلكترونية"

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5.18)، والذي يبين أن الوزن النسبي لجميع فقرات المجال أكبر من الوزن النسبي المحايد "60%" حيث تراوح الـوزن النسبي بين 53.45 % و76.90% وكذلك بلغت قيمة مستوى الدلالة لكل فقرة أقل من 0.05، والجدول رقم (5.18) يوضح ذلك :

جدول (5.18)

ترتيب كل فقرة من الفقرات المتعلقة بـ " سياسات حماية المعلومات الإلكترونية" تبعاً للمتوسطات الحسابية والوزن النسبي ومستوى الدلالة والترتيب (ن = 58)

م	السؤال	المتوسط الحسابي	الوزن النسبي	قيمة t	مستوى الدلالة	الترتيب
27	يعتمد مركز تكنولوجيا المعلومات سياسات خاصة بأمن المعلومات	3.84	76.90	6.897	0.000	1
28	توجد سياسات خاصة باستخدام التوقيع الإلكتروني في مركز تكنولوجيا المعلومات	2.78	55.52	-1.821	0.074	5
29	تعمل إدارة مركز تكنولوجيا المعلوما بصورة مستمرة على تطوير السياسات الخاصة بالتوقيع الإلكتروني	2.67	53.45	-2.815	0.007	6
30	السياسة الأمنية المتبعة في مركز تكنولوجيا المعلومات تحقق سرية المعلومات	3.79	75.86	7.254	0.000	2
31	توجد سياسات خاصة بأمن المعلومات الإلكترونية معروفة لدى جميع الموظفين	2.98	59.66	-0.136	0.892	3
32	يفتقد المركز إلى سياسة واضحة لحماية خصوصية المراسلات الإلكترونية	2.98	59.66	-0.129	0.898	4
	جميع فقرات المجال الخامس	**19.05**	**63.51**	**2.338**	**0.023**	

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.05) = 2.00

قيمة t الجدولية عند درجة حرية (57) وعند مستوى دلالة (0.01) = 2.66

يتبين من الجدول رقم (5.18) أن الفقرة رقم (27) احتلت المرتبة **الأولى** والمتعلقة بـ " يعتمد مركز تكنولوجيا المعلومات سياسات خاصـة بـأمن المعلومـات " ، وبـوزن نـسبي 76.90%، ويعزو الباحث هذة النتيجة إلى أن مراكز تكنولوجيا المعلومـات تعتمـد سياسـات خاصة بأمن المعلومات.

كما احتلت الفقرة رقم (30) المرتبة **الثانية** والمتعلقة بـ " السياسة الأمنية المتبعة فـي مركز تكنولوجيا المعلومات تحقق سرية المعلومات"، وبوزن نسبي 75.86%، ويعزو البـاحـث النتيجة الجيدة إلى أن مراكز تكنولوجيا المعلومات تتبع سياسة أمنية تحقق سرية المعلومات.

ويلاحظ أن الفقرة رقم (31) احتلت المرتبة **الثالثة** والمتعلقة بـ " توجد سياسات خاصة بآمن المعلومات الإلكترونية معروفة لدى جميع الموظفين"، وبوزن نـسبي 59.66%، ويعـزو الباحث سلبية النتيجة إلى أن سياسات أمن المعلومات غير معروفة لدى جميع الموظفين.

كما يلاحظ أن الفقرة رقم (32) احتلت المرتبة **الرابعة** والمتعلقة بـ " يفتقد المركز إلى سياسة واضحة لحماية خصوصية المراسلات الإلكترونية "، وبوزن نسبي 59.66%، ويعـزو الباحث سلبية الإجابة إلى أن مركز تكنولوجيا المعلومات يفتقد إلى سياسـة واضـحة لحمايـة خصوصية المراسلات الإلكترونية.

وبالنظر إلى الجدول رقم (5.18) نلاحظ أن الفقرة رقم (28) احتلت المرتبة **الخامـسة** والمتعلقة بـ" توجد سياسات خاصة باستخدام التوقيع الإلكتروني في مركز الحاسوب"، وبـوزن نسبي 55.52%، ويعزو الباحث سلبية الإجابة إلى عدم وجود سياسات خاصة باستخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات وهذا يتوافق مع نتيجة الفقرة (38).

واحتلت الفقرة رقم (29) المرتبة السادسة – الأخيرة- والمتعلقة بـ" تعمل إدارة مركز تكنولوجيا المعلوماتبصورة مستمرة على تطوير السياسات الخاصة بالتوقيع الإلكتروني"، حيـث بلغ الوزن النسبي 53.45%، ويعزو الباحث سلبية الإجابة إلـى أن إدارة مراكـز تكنولوجيـا المعلومات لا تعمل على تطوير السياسات الخاصة بالتوقيع الإلكتروني.

وبصفة عامة بلغ المتوسط الحسابي لجميع فقرات المجال الخامس " سياسات حمايـة المعلومات الإلكترونية" تساوي 19.05 والوزن النسبي 63.51% ومستوى الدلالة 0.023 وهو أقل من 0.05 مما يدل على أن مراكز تكنولوجيا المعلومات تمتلك سياسات حماية المعلومـات الإلكترونية وبذلك تعتبر" سياسات حماية المعلومات الإلكترونية" من متطلبات استخدام التوقيع الإلكتروني.

ويعزو الباحث تدني النتيجة إلى وجود قصور في تطوير سياسات حماية أمن المعلومات في مراكز تكنولوجيا المعلومات، ويرى الباحث أن على مراكز تكنولوجيا المعلومات أن تقـوم بتطوير سياسات السرية والخصوصية المستخدمة لديها وأن تقوم بتطبيقها وهـذا يتوافـق مـع دراسة Shalhoub (2006).

- إيجاد معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيـا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين السياسات الأمنية المستخدمة حاليـاً، وللتحقق من ذلك تم استخدام معامل ارتباط بيرسون والجدول رقم (5.19) يوضح ذلك:

جدول (5.19)

يوضح معامل الارتباط بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين السياسات المستخدمة حالياً.

المجال	المجموع
السياسات المستخدمة حالياً	**0.719

* قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.05) = 0.250

** قيمة ر الجدولية عند درجة حرية (56) وعند مستوى دلالة (0.01) = 0.325

يتضح من الجدول رقم (5.19) إلى وجود علاقة ارتباطية موجبة ذات دلالة إحـصائية عند مستوى دلالة 0.01 بين متطلبات استخدام التوقيع الالكتروني في إدارة مراكـز تكنولوجيـا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين السياسات المستخدمة حالياً مما يعنـي قبول الفرضية أي انه كلما زاد تطوير السياسات الأمنية المستخدمة حالياً زاد استخدام التوقيـع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة.

ويعزو الباحث ذلك إلى أن استخدام السياسات الأمنية في مراكز تكنولوجيا المعلومات وتطويرها بشكل مستمر سوف يقلل من مخاطر كشف المعلومات ويزيد من حماية خصوصية المستخدمين، وقد اتفقت نتيجة هذه الدراسة مع دراسـة Godwin (2001) حيـث ان الاهتمـام الأساسـي للمتسوقين عبر الإنترنت هي الأمن وحماية الخصوصية أثناء التسوق عبر الإنترنت.

وبهذا يكون الباحث قد تحقق من عدم صحة الفرض الخامس من فروض الدراسة والـذي نص على: لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بـين

متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيـا المعلومـات فـي الجامعـات الفلسطينية في قطاع غزة وبين السياسات المستخدمة حالياً.

وعليه يقبل الباحث بالفرض البديل، حيث تبين وجـود علاقـة ارتباطيـة ذات دلالـة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين السياسات المستخدمة لحماية المعلومات الإلكترونية.

إجمال نتائج مجموع مجالات الإستبانة موضحاً في الجدول رقم (5.20) على النحو التالي:

جدول (5.20)

مجموع مجالات الإستبانة

المجالات	عدد الفقرات	مجموع الاستجابات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي
المجال الأول: تطوير البنية التحتية لمركز تكنولوجيا المعلومات	7	1372	23.66	4.40	67.59
المجال الثاني: اهتمام الإدارة العليا لمركز تكنولوجيا المعلومات باستخدام التوقيع الالكتروني	9	1718	29.62	6.35	65.82
المجال الثالث: وجود المتطلبات القانونية والتشريعية لاستخدام التوقيع الالكتروني	5	1048	18.07	3.98	72.28
المجال الرابع: اعتماد المراسلات الالكترونية	5	996	17.17	4.07	68.69
المجال الخامس: سياسات حماية المعلومات الإلكترونية	6	1105	19.05	3.43	63.51
المجموع	**32**	**6239**	**107.57**	**16.58**	**67.23**

بالنظر إلى الجدول رقم (5.20) نلاحظ أن إجمالي الوزن النـسبي لجميـع المجـالات 67.23% وهى تعتبر نسبة متدنية نوعاً ما حيث أن حماية المعلومات الإلكترونية تعتبـر مـن المهام الرئيسية لمراكز تكنولوجيا المعلومات في الجامعات الفلسطينية، فهذة النسبة تدل على أن حماية المعلومات الإلكترونية والمحافظة على سريتها في هذة المراكز بحاجة إلى تطوير البنيـة التحتية وإلى زيادة الإهتمام من قبل الإدارة العليا لهذة المراكز بالإضافة إلى تطوير الـسياسات الخاصة لحماية أمن المعلومات.

الفصل السادس

برنامج التوقيع الإلكتروني
Digital Signature program

برنامج التوقيع الإلكتروني
Digital Signature program

قام الباحث بإنشاء برنامج لتطبيق التوقيع الإلكتروني للإستخدام الفردي كمبادرة لإدخال التوقيع الإلكتروني في المراسلات الإلكترونية على أن يتم تطوير البرنامج واستخدامة على مستوى المؤسسة الواحدة.

مقدمة عن التطبيق

صمم هذا البرنامج كتطبيق مباشر لفكرة التوقيع الالكتروني حيث تم تطبيقه على المستوى الفردي كمرحلة أولى مع توفر الإمكانية لتطويره وتطبيقه على مستوى القسم في المؤسسة الواحدة -كمرحلة ثانية- (مثل مركز تكنولوجيا المعلومات في الجامعات) ليعمل على مبدأ حماية المراسلات الالكترونية الداخلية، ففي المرحلة الأولى فإن هذا التطبيق يقوم بعملية توقيع المستندات النصية فقط (Text Files) حيث يتم يتم تخزين المستند المُوقع إلكترونياً (لدى المرسل أو المستقبل) على جهاز الحاسوب الشخصي، بحيث يمكن تخزينة كملف نصي على أي جهاز أخر، ولقد تم تطبيق البرنامج في فترة زمنية تقدر بأسبوعين للتحقق من فعالية التطبيق.

في حال نجاح المرحلة الثانية يتم تطبيقه على المؤسسة ككل (مثل مركز تكنولوجيا المعلومات وباقي دوائر وأقسام الجامعة) و يمكن أن يتم تعميم التطبيق ليشمل المراسلات الخارجية للمؤسسة في حال اعتماد تشريع خاص بالتوقيع الالكتروني.

هذا ومن الجدير بالذكر أن هذا التطبيق يعد من التجارب الأولى على مستوى التطبيق الفردي التي أجريت في قطاع غزة حيث من السهولة إضافة تعليمات أخرى Functions بحيث يمكن للبرنامج أن يتعامل مع نوعيات ملفات أخرى مختلفة.

6.1 الأدوات المستخدمة لإنشاء التطبيق

لأن تطبيق فكرة التوقيع الالكتروني تعتمد على خوارزميات رياضية طويلة ومعقدة و تحتاج للكثير من العمليات الحسابية لذلك تم انتاج التطبيق بلغة C++.

كذلك تم استخدام قاعدة البيانات Ms. Access حيث أنها مناسبة للاستخدام الشخصي في المرحلة الأولى في التطبيق وذلك لبساطتها وسهولة التعاملة معها ومتوفرة من خلال حزمةMicrosoft Office الشهيرة.

6.2 التقنيات المستخدمة

يقوم التطبيق على استخدام معادلات الـHashing والتشفير موقع (williamstallings.com)، والتي سنستعرضها في الأسطر القادمة:

أولاً: تقنية الـ Hashing :

يوجد العديد من التقنيات والخوارزميات الرياضية المختلفة لتطبيق مبدأ الـ Hashing، وتتميز كل طريقة بميزات وينقص من شأنها بعض العيوب وفيما يلي ذكر لأهم هذه الطرق مع ميزات وعيوب كل طريقة:

1. Snerfu:

صممت هذه التقنية من قبل رالف ميركل ومن اهم **ميزاتها**:

1. تستخدم 128Bit أو 256Bit كأساس لنتيجة عملية Hashing
2. تعتمد في الأساس على عملية XOR كعملية حسابية مما يعكس بساطة هذه التقنية.

عيوبها:

1. كثرة المخرجات المتطابقة لمدخلات مختلفة وهو ما يعرف بالHashing Birthday

2. MD2, MD4, MD5:

صممت هذه التقنية من قبل روناد ريفست، وتستخدم من قبل شركة مايكوسوفت فـي تطبيقـات الانترنت الخاصة بها، ومن اهم **ميزاتها**:

1. بساطة تطبيق هذه الطريقة و سرعة أدائها.
2. تستخدم 128BIT كأساس لنتيجة عملية Hashing
3. يستخدم 4 دورات حسابية لحساب الناتج.

عيوبها:

1. طول الHashing الناتج باستخدام هذه الطريقة.
2. وجود المخرجات المتطابقة لمدخلات مختلفة وهو ما يعرف بـالHashing Birthday وإن كان بدرجة اقل من الSnerfu ولقد تم تطوير هذه التقنية ثلاث مرات للتقليل مـن هذه المشكلة ، حيث كان أكثرها هو MD2 و أقلها حدوثا MD5.
3. ضعف الناحية الأمنية للبيانات وهذه كانت واضحة فـي MD2 لتختفـي فـي MD4 وMD5

SHA1 .3

حيث تم تصميمه من قبل مؤسستي NIST و NSA التابعتين للفيدرالية الأمريكية، وتشبه بدرجة كبيرة تقنية الMD5 ومن أهم **ميزاتها:**

3. تستخدم 160Bit كأساس لنتيجة عملية Hashing
4. تتميز باستحالة وجود المخرجات المتطابقة لمدخلات مختلفة وهو ما يعرف بالـ Hashing Birthday.
5. قوة الناحية الأمنية للبيانات.

هذا و لقد تم اعتماد هذه التقنية(**SHA1**) في تطبيقنا هذا لما تتمتع به من ميزات وعدم وجود عيوب لها كما في التقنيات الأخرى.

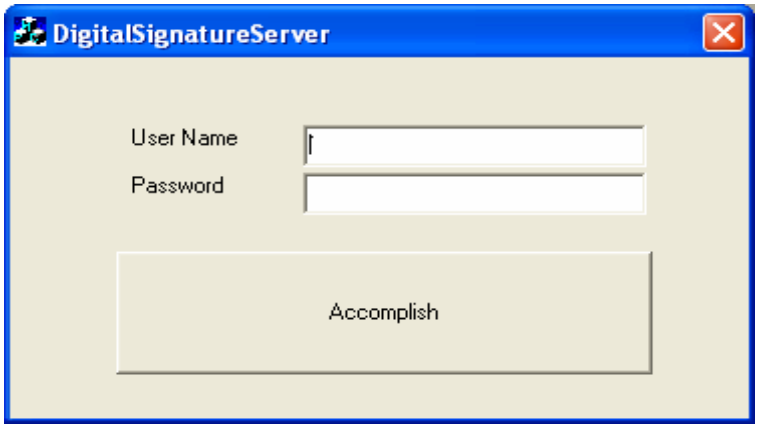
ثانياً: تقنية التشفير:

لقد تم اعتماد تقنية الRSA في تطبيقنا لتقنية التوقيع الإلكتروني وذلك لبساطتها ولصعوبة اختراقها الأمني، حيث تعتمد هذه التقنية على استخدام مفتاحين : مفتاح خاص لتشفير الرسالة يملكه فقط صاحب التوقيع الالكتروني، ومفتاح عام يملكه كل من له صلاحيات قراءة الرسالة.

6.3 وصف التطبيق

يتكون التطبيق من جزأين أساسيين:

1. **مصدر الشهادات:** وهذا التطبيق يقوم بإنشاء المفتاح الخاص والمفتاح العام متضمناً الشهادة الرقمية.



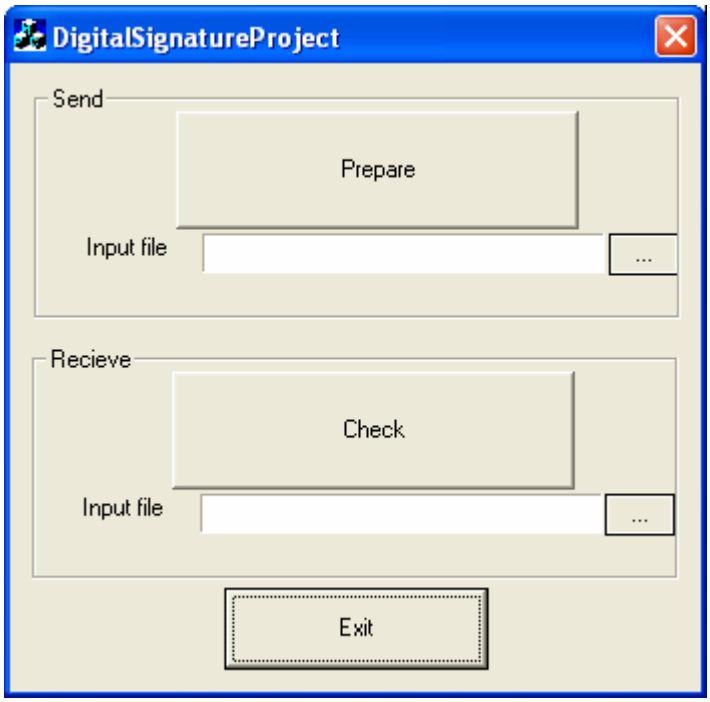
شكل رقم (6.1)

واجهة البرنامج لإصدار المفتاح الخاص والعام متضمناً الشهادة الرقمية

يعمل هذا التطبيق من خلال خادم رئيس يحتوي على قاعدة بينات الـشهادات الرقميـة الداخلية وكذلك يعمل على إنشاء زوج المفاتيح الخاص بالتوقيع الإلكتروني (المفتاح العـام والمفتاح الخاص).

♦ **كيفية إنشاء زوج المفاتيح والشهادة الرقمية:** يقوم مدير التطبيق كما هو موضح بالـشكل رقم (6.1) بإدخال اسم المستخدم في خانة الـ User Name وكلمة المرور في خانـة الـ Password، فيتم الدخول إلى البرنامج لإنشاء مفاتيح التوقيع الإلكترونـي متـضمنة الـشهادة الرقمية كما هو موضح في الشكل رقم (6.2)، ومن ثم الضغط على زر Accomplish حيـث يقوم التطبيق بإنشاء زوج المفاتيح مع الشهادة الرقمية باسم المستخدم المقصود وبشكل مرن.

2. **برنامج التوقيع الالكتروني:** وهذا التطبيق يقوم بعمل الـ digest للرسالة ومن ثم تشفيرها باستخدام المفتاح الخاص وأيضا استقبال الرسالة وفك تشفيرها باستخدام المفتاح العام.



شكل رقم (6.2) واجهة البرنامج لدى المرسل والمستقبل للرسالة

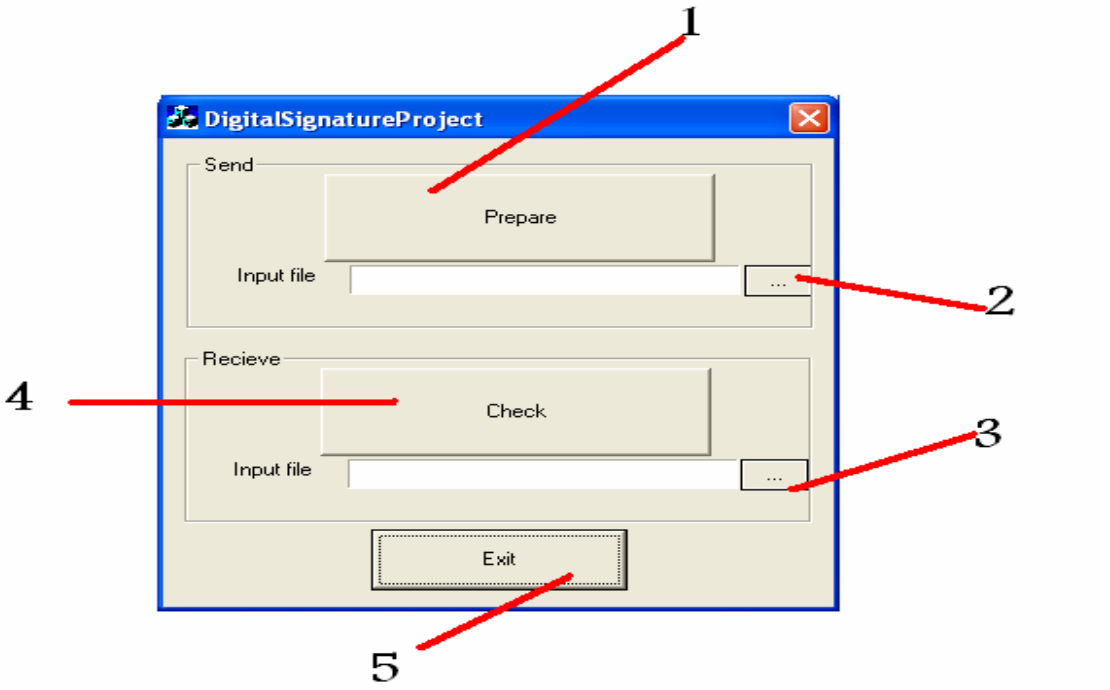
كما هو مبين من الأشكال (6.1) و (6.2) فإن هذا التطبيق يـستخدم بـسهولة وبـنفس طريقة عمل الكثير من التطبيقات المنتشرة التي تعمل على الكمبيوتر الشخصي للمستخدم لبرامج تشغيل شركة ميكروسوفت.

6.4 كيفية تشغيل البرنامج:

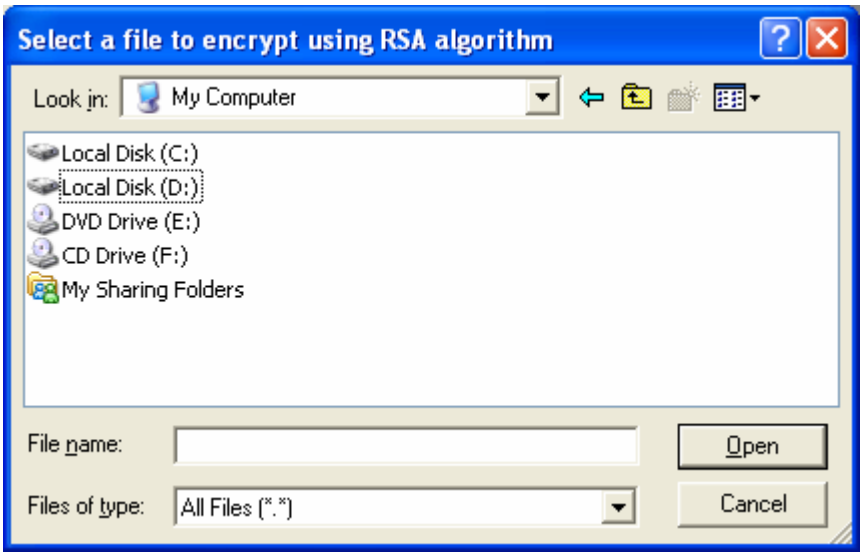
يتم الدخول باستخدام اسم مستخدم/ كلمة مرور خاصة بكل مستخدم يتم منحه إياها من قبل مدير التطبيق، الشكل التالي يوضح باب الدخول للبرنامج:

شكل رقم (6.3) واجهة الدخول للبرنامج لدى المستخدم

1. **الإرسال** : تنفذ عملية إرسال المستند عبر البرنامج باستعراض الملفات زر رقم (2) لاختيار المستند المقصود توقيعة ومن ثم إرساله كما هو موضح في الشكل رقم (6.4)



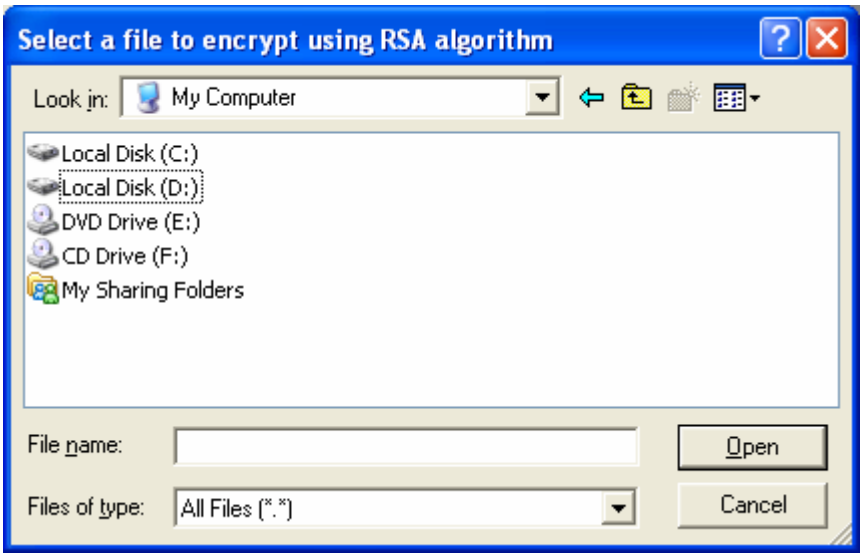
شكل رقم (6.4) واجهة إرسال واستقبال الستند لتوقيعه وللتحقق من التوقيع



شكل رقم (6.5) واجهة البرنامج لإستعراض الملفات لإختيار المستند المطلوب توقيعة

يختار المستخدم الملف المطلوب ثم يضغط على زر رقم (1) والذي يقـوم بتجهيـز الرسـالة والتوقيع الخاص بها ويحفظها في نفس المكان بامتداد (.out) ليتم إرسالها لاحقاً.

3. **الاستقبال** : وذلك من خلال اختيار ملف الرسالة بالضغط على زر رقم (3) كما في الشكل رقم (6.4) لاستعراض الملفات والموضح من خلال الشكل رقم (6.6) التالي:



شكل رقم (6.6) واجهة إستعراض الملفات لإختيار المستند المطلوب التحقق من توقيعه

يختار المستخدم ملف الرسالة المشفرة المطلوب ثم يضغط على زر رقم (4) كما في الشكل رقم (6.4) والذي يقوم بفحص الرسالة وفك التشفير الخاص بها في نفس اللحظة، وفي حال وجود أي تغيير أو تحريف على الرسالة فإن البرنامج يوضح ذلك في الحال.

الخلاصة:

إن استخدام برنامج التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات يعمل على حماية المراسلات الإلكترونية والحفاظ على الخصوصية للبيانات الإلكترونية داخل الحـرم الجـامعي، حيث أن هذة التقنية كما بينت نتيجة الدراسة لم تكن مستخدمة من قبل في مراكـز تكنولوجيـا المعلومات فإنها بذلك تعتبر إضافة نوعية لحماية المعلومات الإلكترونية في مراكـز تكنولوجيـا المعلومات في الجامعات الفلسطينية في قطاع غزة.

الفصل السابع

أولاً:النتائج

ثانياً:التوصيات

ثالثاً: الدراسات المقترحة

النتائج والتوصيات

أولاً: نتائج الدراسة

1. مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة لا يتوفر فيها موظف بمسمى وظيفي " مدير امن المعلومات".
2. 72.41% من موظفي مراكز تكنولوجيا المعلومات لم يسبق وان استخدموا التوقيع الإلكتروني.
3. 74.14% يؤيدون أن استخدام التوقيع الإلكتروني بين المؤسسات التعليمية بحاجة إلى استصدار تشريع من المجلس التشريعي لأستخدامه.
4. 51.72% يعتقدون انه لا يوجد توجه لإستخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات.
5. 32.76% من موظفي مراكز تكنولوجيا المعلومات ذات العلاقة بعملهم يعتقدون أنه تم اختراق أنظمة الحاسوب في الجامعة.
6. 60.34 % لا يوجد إجراءات دورية ومحددة يقوم بها مدير أمن المعلومات في المركز (أو من ينوب عنه) للحفاظ على أمن المعلومات.
8. تقنية التوقيع الإلكتروني لا تستخدم في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية.
9. المعدات والبرمجيات الأمنية المستخدمة في مراكز تكنولوجيا المعلومات بحاجة إلى تحديث وتطوير لتواكب التقنيات العالمية المتطورة في مجال امن المعلومات.
10. موظفي مراكز تكنولوجيا المعلومات بحاجة إلى مزيد من التدريب المستمر لتطوير برمجيات متخصصة بأمن المعلومات تكون قادرة على حماية المعلومات الإلكترونية.
11. موازنة مراكز تكنولوجيا المعلومات لا تتضمن تطوير وتحديث تقنيات أمن المعلومات المستخدمة في مراكز تكنولوجيا المعلومات.
12. إدارة مراكز تكنولوجيا المعلومات لا تعمل ضمن خطة إستراتيجية واضحة مما يعني إلى عدم وضوح الرؤية المستقبلية لإدارة مراكز تكنولوجيا المعلومات.
13. الشهادات الرقمية غير معتمدة للخادم الرئيسي في مراكز تكنولوجيا المعلومات وفي المراسلات الإلكترونية.

14. 78.62 % من المستبانين يعتقدون أن استخدام التوقيع الإلكتروني بين أقسام ودوائر الجامعة يحتاج إلى اعتماد الإدارة العليا للجامعة وليس لإستصدار قانون تشريعي من المجلس التشريعي لإعتماده.
15. إدارة مراكز تكنولوجيا المعلومات هي الجهة المبادرة والمتخصصة التي توصي باستخدام التوقيع الإلكتروني في المراسلات الإلكترونية بين دوائر وأقسام الجامعة.
16. 72.76% يعتقدون أن اعتماد المراسلات الإلكترونية الرسمية بين أقسام ودوائر الجامعة بحاجة إلى اعتماد الإدارة العليا للجامعة.
17. 71.72% يؤيدون توفر الإمكانيات التقنية في مراكز تكنولوجيا المعلومات لحفظ واعتماد المراسلات الإلكترونية.
18. مراكز تكنولوجيا المعلومات تفتقر إلى سياسات واضحة لحماية خصوصية المراسلات الإلكترونية.
19. إدارة مراكز تكنولوجيا المعلومات لا تعمل بصورة مستمرة على تطوير السياسات الخاصة بأمن المعلومات.
20. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين معوقات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين تطوير البنية التحتية لمراكز تكنولوجيا المعلومات.
21. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين معوقات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اهتمام الإدارة العليا باستخدام التوقيع الإلكتروني.
22. توجد علاقة بين معوقات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين وجود المتطلبات القانونية والتشريعية لاستخدامه
23. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$ بين معوقات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين اعتماد المراسلات الإلكترونية "
24. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين معوقات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة وبين السياسات المستخدمة لحماية المعلومات الإلكترونية.

ثانياً: التوصيات

في نهاية هذه الدراسة ومن خلال أدبيات الدراسة التي تعرض لها الباحث، بالإضـافة إلـى الجانب العملي وما تضمنته من نتائج الاستبانات، خلص الباحث إلى التوصيات التالية :-

- مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية بحاجة إلى تعيين موظف بمـسمى مدير أمن المعلومات.
- إنشاء دائرة حماية المعلومات تعمل على تطبيق حماية الخصوصية
- العمل على استخدام تقنية التوقيع الإلكتروني فـي المراسـلات الإلكترونيـة لمراكـز تكنولوجيا المعلومات في الجامعات الفلسطينية.
- اصدار قانون تشريعي من المجلس التشريعي الفلسطيني لحماية التوقيع الإلكتروني بـين المؤسسات المختلفة.
- تحديث المعدات الأمنية المستخدمة حالياً في مراكز تكنولوجيا المعلومات في الجامعـات الفلسطينية.
- تطوير برمجيات أمن المعلومات لتكون قادرة على حمايـة المعلومـات فـي مراكـز تكنولوجيا المعلومات في الجامعات الفلسطينية بكفاءة.
- التدريب المستمر لموظفي مراكز تكنولوجيا المعلومات في الجامعات الفلـسطينية فـي مجال أمن المعلومات.
- تدريب موظفي قسم البرمجة في مراكز تكنولوجيا المعلومات في الجامعات الفلـسطينية على إنشاء وتطوير برمجيات متخصصة بأمن المعلومات لتكون قـادرة علـى حمايـة المعلومات الإلكترونية.
- تحفيز وتشجيع موظفي مراكز تكنولوجيا المعلومات في الجامعـات الفلـسطينية علـى الإطلاع ومتابعة تطورات أمن المعلومات.
- عقد ورشات ولقاءات علمية متخصصة باشتراك خبراء وكفاءات أكاديمية وتقنية بـأمن المعلومات بصورة مستمرة لموظفي مراكز تكنولوجيـا المعلومـات فـي الجامعـات الفلسطينية.
- تضمين الموازنة السنوية لمراكز تكنولوجيا المعلومات في الجامعات الفلسطينية لتحديث وتطوير معدات وبرمجيات أمن المعلومات

- تخصيص موازنة سنوية خاصة بتدريب موظفي مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية.
- نوصي إدارة الجامعات الفلسطينية إلى اعتماد المراسلات الإلكترونية باستخدام التوقيع الإلكتروني في المراسلات الرسمية الداخلية بين جميع أقسام ودوائر الجامعات.
- تعيين المتخصصين في مجال تكنولوجيا المعلومات في الإدارة العليا لمراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة.
- وضع خطط تدريبية ومتابعة طبيقها في مجال أمن المعلومات بصورة مستمرة لتطوير موظفي مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية.
- وضع خطة استراتيجية واضحة لمراكز تكنولوجيا المعلومات والعمل وفق هذة الخطة.
- العمل على تطوير سياسات أمن المعلومات ضمن الخطة الإستراتيجية لمراكز تكنولوجيا المعلومات في الجامعات الفلسطينية.
- العمل على إنشاء البنية التحتية لتقنية التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات.
- وضع سياسات واضحة لحماية خصوصية المراسلات الإلكترونية.
- وضع السياسات الخاصة باستخدام التوقيع الإلكتروني.
- اعتماد الشهادات الرقمية للخادم الرئيس وللمراسلات الإلكترونية في مراكز تكنولوجيا المعلومات.
- توضيح سياسات أمن المعلومات لموظفي مراكز تكنولوجيا المعلومات.
- تطوير سياسات أمن المعلومات بصورة مستمرة في مراكز تكنولوجيا المعلومات.

مقترحات الدراسة:

يقترح الباحث أن تقوم مراكز تكنولوجيا المعلومات بإنشاء قسم بمسمى" قسم أمن المعلومات الإلكترونية" مع توفير موظف بمسمى وظيفي " مدير امن المعلومات" لحماية البيانات الإلكترونية من الكشف والتزوير ووضع الخطط الوقائية للحيلولة دون اختراق أنظمة المعلومات الإلكترونية في هذة المراكز، والعمل على تطوير الكادر البشري بشكل مستمر لمواكبة التطورات التقنية المتسارعة في مجال تكنولوجيا المعلومات، بالإضافة إلى العمل بشكل مستمر لتحديث وتطوير معدات وبرمجيات أمن المعلومات الإلكترونية.

ثالثاً: الدراسات المقترحة :

- إدارة أمن المعلومات في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية
- واقع استخدام التوقيع الإلكتروني في مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في ظل استخدام تقنية التوقيع الإلكتروني.

المراجـــــــــع

أولا: المراجع العربية

ثانياً: المراجع الإنجليزية

المراجع:

تم تصنيف المراجع وفق الترتيب التالي : (الكتب ، ثم أوراق العمل والدوريات والمجـلات ، ثـم الدراسـات العلمية، ثم مواقع على الإنترنت) .

أولاً: المراجع العربية:

- داود، حسن طاهر،(2004)، "**أمن شبكات المعلومات"،** مركز البحوث-معهد الإدارة العامة، صفحة206 ،الرياض، السعودية.

- دليل" إدارة تكنولوجيا المعلومات"، 2005، الجامعة الإسلامية، غزة، فلسطين.

- الدليل العام لجامعة الأزهر 2004، غزة، فلسطين.

- دليل جامعة الأقصى 2005- 2006، غزة، فلسطين.

- عبيدات، ذوقات، عبد الرحمن عدس، كايد عبد الحق(2001)، " **البحث العلمي، مفهومه وأدواته وأساليبه**" ، دار الفكر للنشر والتوزيع، عمان، الأردن.

- المطالقة، محمد فواز (2006)، "**الوجيز في عقود التجارة الإلكترونية: أركانه، إثباته، القانون الواجب التطبيق ، حمايته"التشفير، التوقيع الإلكتروني"و دراسة مقارنه"،** دار الثقافة للنشر والتوزيع، الطبعة الأولى/الإصدار الأول، 2006، عمان، الأردن.

- المومني، عمر حسن(2003)، "**التوقيع الإلكتروني وقانون التجارة الإلكترونية – دراسة قانونية وتحليلية مقارنة"،** دار وائل للنشر والتوزيع، الطبعة الأولى، عمان، الأردن.

- نصيرات، علاء محمد(2005)، "**حجية التوقيع الإلكتروني في الإثبات– دراسة مقارنة**"،رسالة ماجستير، دار الثقافة للنشر والتوزيع، الإصدار الأول، 2005، عمان، الأردن.

ثانياً: المراجع الإنجليزية:

Borasky, Danielle V. ,(1999), **"Digital Signatures",** Jul/Aug 99, vol.23, Issue 4, P47, 4P, 1 diagram. ISSN: 0146-5422.

CGI,(2004**),"Public Keys Encryption and digital signature: How do they work?"**
http://www.cgi.com/web/en/library/white_papers/p1.htm

Christopher Ashley, (2007**), "MEMORANDUM** :**E-Signatures in University Transactions",** www.uww.edu/Adminforms/esigauthor.doc , (last Access 1 March 2007).

David C. Chou, David C. Yen, (2001**)," intranets for organizational innovation",** Information Management & Computer Security, 2001, Vol. 9/2, P80- 87**.**

Department of Information Resources ، **(**2002**), "Guidelines for the Management of Electronic Transactions and Signed Records",** Prepared by the UETA Task Force of the Department of Information Resources and the Texas State Library and Archives Commission ,September 2002.
http://www.tsl.state.tx.us/slrm/recordspubs/UETA_guidelines.doc

Edward H. , Freeman J.D. ,(2004)**"Digital Signatures and Electronic Contracts",** Information Systems Security , May/June 2004.

Fredric G., (1994**),"Protection of Electronic Mail and electronic Messages Challenges and Solutions",** Security and Control Products, Nashua, New Hampshire,USA.

Gabor Moroc, (2004), "**Summary of Current Law on Electronically Generated and Digital Signatures"** , http://www.csdaca.org/conferences/Automation%20impacts%20on%20Attorney%20Ethical%20Issues_MCLE/DCSS%20Digitizd%20signature%20Summary.do (Last Access Marsh 2007)

Godwin J. Udo, (2001**)," Privacy and Security concerns as major**

barriers for e-commerce: a survey study", Information Management & Computer Security, 2001, Vol. 3/8 , P143-13**.**

Vesna Hassler, Helmut Biely, (1999)," **Digital Signature Management**", Electronic Networking Applications and Policy, Volume 9 Number 4,1999 pp. 262-271, ISSN 1066-2243

Mike Horton, Clinton Mugge ,(2003**), " Hack Note**s, Network Security – Potable Reference **"**, McGraw-Hill companies, ISBN: 0-07-2227883-4, USA.

Jones, Jennifer, Johnston, Margret, (2000), "**Digital signature bill enables e-commerce",** InfoWorld; 06/19/2000, Vol. 22 Issue 25, p8, 1/2p, 1diagram.

Judith V. Boettcher and Amanda Powell **,** "**Digital Certificates, What Are They, and What Are They Doing in My Browser?"** www.cren.net/crenca/docs/syllabus.doc **,** (last Access March 2007)

Kostas Moulinos & others,(2004),**"Towards Secure sealing of Privacy Policies",** Information Management & Computer Security, Volume 14 Number 2, 2006 pp. 104-115, Emerald Group Publishing limited, 0968-5227.

Kuechler W. , Grupe F. ,(2002),**"Digital Signatures: A Business View",** Information System Security, Mar/April 2002, Vol.11 Issue 1, P23, 13P.

Kwo-shing Hong & others, (2006), **"An empirical study of information security policy on information security elevation in Taiwan",** Information Management & Computer Security, Volume 12 Number 4, 2004 pp. 350-361, Emerald Group Publishing limited, 0968-5227.

Meckbach, Greg, (1998),**"Digital signature reaches new level",** Computing Canada; 06/22/98, Vol. 24 Issue 24, p13, 2p, 1c.

Minihan, Jim , (2001),**"Electronic Signature Technologies: A Tutorial"**, Information Management & Computer Security, Volume 9 Number 4 2001 pp. 165-174, ISSN 0968-5227.

Radcliff, Deborah, (2000**),"Digital Signatures"**, Computerworld; 4/10/2000, Vol. 34 Issue 15, p64, 1p.

Rodney J. Petersen, (2004), " **A Framework for IT Policy Development"** *Educause Review*, vol. 39, no. 2 (March/April 2004): P54–55. http://www.educause.edu/apps/er/erm04/erm0428.asp

Stephen Wilson, (1999), **"Digital Signatures and the Future of Documentation",** Information Management & Computer Security, Volume 7 Number 2 1999 pp. 83-87, ISSN 0968-5227.

Whitaker, David, (2007**), "E-Signatures in the Higher Education Environment", www.abanet.net** ، (last Access 1 March 2007).

White, Ron, (2000), **"Digital signatures",** PC Computing; Mar2000, Vol. 13 Issue 3, p152, 2p, 4c, ISSN: 0899-1847.

Yakal, Kathy, (2000), "**Make Approvals Bulletproof",** PC Magazine; 09/19/2000, Vol. 19 Issue 16, p34, 1/3p.

- الأونسيترال ,لجنة الأمم المتحدة للقانون التجاري الدولي
http://www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/1996Model.html ,(Last Access Nov.2007).

- موقع (Wikipedia)
http://en.wikipedia.org/wiki/digital_signature (Last access March 2007).

- موقع (entrust)
http://www.entrust.com/digitalsig/description.htm (Last access April 2007)

- جامعة الأقصى
http://www.alaqsa.edu.ps/arabic/ccenter/default.asp , (Last access April 2007)

- الجامعة الإسلامية- غزة
http://www.iugaza.edu.ps/ara/it/ (Last access April 2007)

- جامعة الأزهر
  http://www.alazhar.edu.ps/arabic/Centers/Information_Technology_Unit/ITU.htm (Last access April 2007)

- جامعة القدس المفتوحة

  http://www.qou.edu/homePage/arabic/index.jsp?pageId=93, (Last access April 2007)

- موقع شركة (Teletrust)

www.teletrust.de/fileadmin/files/AG7_Flyer2001_e_24.doc ,(Last access April 2007)

- موقع شركة (Microsoft)
  http://support.microsoft.com/kb/195724 ,Article ID 195724, Last Review January 23, 2007, (Last access Septemper 2007).

- موقع شركة (IBM)
  http://www.ibm.com/developerworks/lotus/library/securemessaging/

- موقع شركة (entrust)
  www.entrust.com/resources/pdf/cryptointro.pdf - 2007-01-23

- North Carolina University
  http://www.unc.edu/~dvb/cyberlaw/digitalsignatures/security.htm#Advanatges , (Last access April 2007).

- University of Michigan

  "**Guidelines for Implementing the Proper Use Policy of the University of Michigan: Responsible Use of Technology Resources**" , December 2002, http://spg.umich.edu/ , (last Access 1Sep. 2007).

- University of New York
  "**State University of New York at Stony brook responsible use of information technology policy**", April 2001, http://naples.cc.sunysb.edu/Admin/policy.nsf/pages/P109#web#web (last Access 1Sep. 2007).

- Michigan Technological University
  http://www.cs.mtu.edu/~yinma/Index.html (last Access 11Nov. 2007).

- Arizona State University
  www.asu.edu/ecure/2002/dollar/index.html

- http://www.definethat.com/define/5691.htm

- http://computer.howstuffworks.com/question571.htm ,(Last access February 2007).

- http://www.us-cert.gov/cas/tips/ST04-018.html ,(Last access march 2007)

- www.e-signature.gov.eg/materials/hwhab_e-signatuere_different.ppt (Last access April 2007)

- http://searchsecurity.techtarget.com/sDefinitiion/0,,sid14_gci11953,00.html (Last access April 2007)

- http://pr-qa.com/solutions/qacpp_benefits2.htm

- http://williamstallings.com/Extras/Security-otes/lectures/authent.html#fn

ملاحق الدراسة

- استبانة الدراسة
- كود التطبيق لبرنامج التوقيع الإلكتروني

ملحق رقم (1)

الجامعة الإسلامية غزة **رقم الاستبانة: ــــــــ**

عمادة الدراسات العليا

كلية التجارة - إدارة الأعمال

استبانة لمعرفة

متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة

الأخ الفاضل... الأخت الفاضلة..

يسعى الباحث في هذة الإستبانة إلى التعرف على **متطلبات استخدام التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة.**

ولإيماننا العميق بأنكم الأكثر معرفة بالوضع القائم في مركزكم، وأنكم خير مصدر للوصول إلى المعلومات المطلوبة، كونكم أهـل خبـرة واختصاص، ونعهد بكم الاهتمام والاستعداد الدائمين لمؤازرة الأبحاث العلمية، التي تخدم المجتمع وتطوره، لذا توجهنـا إلـيكم لتعبئـة هـذة الإستبانة وكلنا امل ان نجد التعاون المطلق من قبلكم.

علماً ان حرصكم على تقديم المعلومات الكافية **بدقة وموضوعية** سيؤدي إلى – بدون شك- الوصول إلى أفضل النتائج لموضوع الدراسة، مما سيعود بالنفع والخير لما فيه مصلحة لجامِعاتُنا بإذن الله .

ملاحظة: البيانات التي يتم الحصول عليها منكم تستخدم فقط لأغراض البحث العلمي ويراعى فيها السرية التامة، حيث لا يتم التصريح باسم أية مركز لتكنولوجيا المعلومات(مركز الحاسوب) عند الحديث عن النتائج.

الرجاء وضع حرف x في المربع المرتبط بإجابتك.

وتشكركم لحسن تعاونكم،،،

الباحث: صلاح عبد الحكيم المصري
إشراف كل من: د.عصام البحيصي – كلية التجارة
د.توفيق برهوم – كلية تكنولوجيا المعلومات

استخدام التوقيع الإلكتروني

أولا: معلومات عامة

1- الجنس

☐ ذكر ☐ أنثى

2- إسم الجامعة:

☐ الإسلامية ☐ الأزهر ☐ الأقصى ☐ القدس المفتوحة ☐ فلسطين

3- المؤهل العلمي.

☐ ثانوية فما دون ☐ دبلوم ☐ بكالوريوس ☐ دراسات عليا

4- التخصص.

☐ هندسة حاسوب ☐ علوم كمبيوتر ☐ تكنولوجيا معلومات ☐ غير ذلك(الرجاء حدد)

- - - - - - - - - - -

5- عمر مركز تكنولوجيا المعلومات .

☐ أقل من سنتين ☐ سنتان - 5 سنوات ☐ 6 - 10 سنوات ☐ أكثر من 10 سنوات

6- عدد سنوات الخبرة في مجال تكنولوجيا المعلومات.

☐ أقل من سنتين ☐ سنتان – 5 سنوات ☐ 6 – 10 سنوات ☐ أكثر من 10 سنوات

7- المسمى الوظيفي (اختر اجابة واحدة فقط من فضلك).

☐ رئيس مركز تكنولوجيا المعلومات ☐ مدير دائرة ☐ رئيس قسم ☐ مدير أمن المعلومات

☐ مدير قواعد البيانات ☐ مدير الأنظمة ☐ مدير الشبكة ☐ صيانة حاسوب ودعم فني

☐ محلل نظم ☐ مصمم صفحات إنترنت ☐ مبرمج ☐ غير ذلك (الرجاء حدد):- - - - -

8- هل سبق وأن استخدمت التوقيع الإلكتروني؟

☐ نعم ☐ لا

- في حالة الإجابة بـ "نعم" فما هي الفترة الزمنية؟

☐ أقل من سنة ☐ من سنة - سنتين ☐ 2 - 5 سنوات ☐ أكثر من 5 سنوات

9- هل المؤسسات التعليمية بحاجة إلى استصدار تشريع من قبل المجلس التشريعي للسماح باستخدام التوقيع الإلكتروني فيما بينهم وبين المؤسسات الأخرى؟

☐ نعم ☐ لا

10- هل هناك توجه لإستخدام التوقيع الإلكتروني في مركز تكنولوجيا المعلومات ؟

☐ نعم ☐ لا

11- هل سبق وأن تم إختراق أنظمة الحاسوب في الجامعة مسبقاً ؟

☐ نعم ☐ لا ☐ ليس ضمن مجال عملي

في حالة الإجابة بـ "نعم" فإن السبب يرجع إلى: (يمكن أختيار أكثر من إجابة مع مراعاة الترتيب حسب الأهمية):

☐ أنظمة الحماية المستخدمة بحاجة إلى تحديث.
☐ ضعف الخبرات التقنية لموظفي مركز تكنولوجيا المعلومات .
☐ عدم توفر الإمكانيات المادية لحماية أمن المعلومات.
☐ عدم توفر المعدات والبرمجيات الخاصة بحماية أمن المعلومات.
☐ امن المعلومات ليس من اهتمام الإدارة العليا لمركز تكنولوجيا المعلومات .
☐ غير ذلك (أذكر السبب):----------

12- هل هناك إجراءات دورية ومحددة يقوم بها مدير أمن المعلومات في المركز للحفاظ على أمن المعلومات (سؤال خاص بمدير أمن المعلومات أو من ينوب عنه) ؟

☐ دائماً ☐ غالباً ☐ أحياناً ☐ نادراً ☐ مطلقاً

13- هل إدارة مركز تكنولوجيا المعلومات تتبع معايير محددة وخاصة بأمن المعلومات يتم تحديثها بشكل مستمر؟

☐ نعم ☐ لا

14- هل برمجيات أمن المعلومات المستخدمة حالياً في المركز من إنتاج قسم البرمجة في المركز ؟

☐ جميعها ☐ بعضها ☐ لا يوجد

ثانيا: مجالات الدراسة

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الأول: تطوير البنية التحتية لمركز تكنولوجيا المعلومات					
.15	يستخدم مركز تكنولوجيا المعلومات تقنيات إلكترونية بديلة عن التوقيع الإلكتروني.					
.16	موازنة مركز تكنولوجيا المعلومات تسمح بإنشاء بنية تحتية لتقنية التوقيع الإلكتروني.					
.17	يدرك موظفو مركز تكنولوجيا المعلومات بأهمية استخدام التوقيع الإلكتروني.					
.18	المعدات الأمنية المستخدمة في مركز تكنولوجيا المعلومات لحماية المراسلات الإلكترونية تواكب التطور التقني.					
.19	البرمجيات الأمنية المستخدمة في مركز تكنولوجيا المعلومات لحماية المراسلات الإلكترونية يتم تحديثها بشكل مستمر.					
.20	موظفو مركز تكنولوجيا المعلومات على اطلاع مستمر بتطور تقنيات أمن المعلومات بشكل عام وبتقنية التوقيع الإلكتروني بشكل خاص.					
.21	موظفو مركز تكنولوجيا المعلومات يمتلكون مؤهلات وخبرات تقنية جيدة في إنشاء تقنيات أمن المعلومات وخاصة تقنية التوقيع الإلكتروني.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الثاني: اهتمام الإدارة العليا لمركز تكنولوجيا المعلومات باستخدام التوقيع الإلكتروني					
.22	استخدام تقنية التوقيع الإلكتروني مدرجة ضمن الخطة الإستراتيجية لمركز تكنولوجيا المعلومات .					
.23	تعمل إدارة مركز تكنولوجيا المعلومات على انشاء البنية التحتية لتقنية التوقيع الإلكتروني.					
.24	إدارة مركز تكنولوجيا المعلومات على اطلاع مستمر بالتطورات التقنية لأمن المعلومات.					
.25	إدارة مركز تكنولوجيا المعلومات على اطلاع بأهمية استخدام التوقيع الإلكتروني.					
.26	إدارة مركز تكنولوجيا المعلومات حريصة على تطوير موظفي المركز بصورة مستمرة في مجال أمن المعلومات.					
.27	تعتمد إدارة مركز تكنولوجيا المعلومات المراسلات الإلكترونية.					
.28	تعتمد إدارة مركز تكنولوجيا المعلومات الشهادات الرقمية (Digital Signatures) للخادم الرئيسي في المركز وللمراسلات الإلكترونية.					
.29	تعمل إدارة مركز تكنولوجيا المعلومات ضمن خطة إستراتيجية واضحة.					
.30	إدارة مركز تكنولوجيا المعلومات قادرة على إدارة المركز بكفاءة					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الثالث:وجود المتطلبات القانونية والتشريعية لاستخدام التوقيع الإلكتروني					
.31	يلزم استصدار تشريع قانوني من المجلس التشريعي يسمح باستخدام التوقيع الإلكتروني بين دوائر الجامعة.					
.32	استخدام التوقيع الإلكتروني بين أقسام ودوائر الجامعة بحاجة إلى موافقة الإدارة العليا للجامعة.					
.33	يعتمد استخدام التوقيع الإلكتروني في المراسلات الإلكترونية بين أقسام مركز تكنولوجيا المعلومات بأخذ موافقة إدارة المركز .					
.34	التوقيع الإلكتروني بحاجة إلى إستصدار قانون تشريعي من المجلس التشريعي لحمايته.					
.35	إبرام العقود الإلكترونية يتم حمايتها قانونياً وتشريعياً.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الرابع: اعتماد المراسلات الإلكترونية					
.36	يتم تبادل المراسلات بين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعة إلكترونياً.					
.37	يتم تبادل المراسلات إلكترونياً بين أقسام مركز تكنولوجيا المعلومات .					
.38	تستخدم تقنية التوقيع الإلكتروني في المراسلات الإلكترونية لمركز تكنولوجيا المعلومات					
.39	تتوفر الإمكانيات التقنية في مركز تكنولوجيا المعلومات لحفظ واعتماد المراسلات الإلكترونية.					
.40	اعتماد المراسلات الإلكترونية بين مركز تكنولوجيا المعلومات والدوائر الأخرى في الجامعة بحاجة إلى اعتماد الإدارة العليا للجامعة.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الخامس : سياسات حماية المعلومات الإلكترونية					
.41	يعتمد مركز تكنولوجيا المعلومات سياسات خاصة بأمن المعلومات.					
.42	توجد سياسات خاصة باستخدام التوقيع الإلكتروني في مركز تكنولوجيا المعلومات .					
.43	تعمل إدارة مركز تكنولوجيا المعلومات بصورة مستمرة على تطوير السياسات الخاصة بالتوقيع الإلكتروني.					
.44	السياسة الأمنية المتبعة في مركز تكنولوجيا المعلومات تحقق سرية المعلومات.					
.45	توجد سياسات خاصة بأمن المعلومات الإلكترونية معروفة لدى جميع الموظفين.					
.46	يفتقد المركز إلى سياسة واضحة ومحددة لحماية خصوصية المراسلات الإلكترونية.					

ملحق رقم (2)

كود التطبيق لبرنامج التوقيع الإلكتروني

7.1 كود التطبيق

أولاً: برنامج اصدار الشهادات الرقمية: ويحتوي على دالة إصدار الشهادات الرقمية حيث يقوم بتوليد المفتاح العام والمفتاح الخاص لإسم المستخدم المدخل كما التالي:

```
void CDigitalSignatureServerDlg::OnAccomplish()
{

UpdateData();
//Step-1 Generating Random Numbers
GeneratePrimeNumbers();

//Step-2 calculating n=p*q
m_n = m_Prime1 * m_Prime2;
//Step-3 0=(p-1)(q-1)
m_Undef = (m_Prime1-1) * (m_Prime2-1);
//Step-4 Selecting 'e'
SelectE();
//m_e=17;
//Step-5 Calculate 'd'
CalculateD();
//Displaying private and public keys
//(1) Public key KU={e,n}

//(2) Private key KU={d,n}

if (ptrCDigitalSignatureDB.IsOpen())
ptrCDigitalSignatureDB.Close();

ptrCDigitalSignatureDB.Open();

ptrCDigitalSignatureDB.AddNew();

ptrCDigitalSignatureDB.m_DS_User=m_UserName;
ptrCDigitalSignatureDB.m_DS_Password=m_Password;
ptrCDigitalSignatureDB.m_DS_d=m_d;

ptrCDigitalSignatureDB.m_DS_e=m_e;
ptrCDigitalSignatureDB.m_DS_n=m_n;
ptrCDigitalSignatureDB.Update();

MessageBox("Done Successfully");

}
```

7.2 برنامج التوقيع الالكتروني ويتكون من أجزاء أساسية وهى:

الـ Class الذي يكون كود الـ Hashing ويتكون من الملفين Sha1.h و الـ Sha1.cpp مفصلين كما يلي:

Sha1.h .a

```
#if !defined(AFX_SHA1_H__892E0361_14F2_4E6C_85C9_853CF05AC5F8__INCLUDED_)
#define AFX_SHA1_H__892E0361_14F2_4E6C_85C9_853CF05AC5F8__INCLUDED_


/*
    100% free public domain implementation of the SHA-1 algorithm
    by Dominik Reichl <dominik.reichl@t-online.de>
    Web: http://www.dominik-reichl.de/

    Version 1.6 - 2005-02-07 (thanks to Howard Kapustein for patches)
    - You can set the endianness in your files, no need to modify the
      header file of the CSHA1 class any more
    - Aligned data support
    - Made support/compilation of the utility functions (ReportHash
      and HashFile) optional (useful, if bytes count, for example in
      embedded environments)

    Version 1.5 - 2005-01-01
    - 64-bit compiler compatibility added
    - Made variable wiping optional (define SHA1_WIPE_VARIABLES)
    - Removed unnecessary variable initializations
    - ROL32 improvement for the Microsoft compiler (using _rotl)

    ======== Test Vectors (from FIPS PUB 180-1) ========

    SHA1("abc") =
        A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D

    SHA1("abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq") =
        84983E44 1C3BD26E BAAE4AA1 F95129E5 E54670F1

    SHA1(A million repetitions of "a") =
        34AA973C D4C4DAA4 F61EEB2B DBAD2731 6534016F
*/

#ifndef ___SHA1_HDR___
#define ___SHA1_HDR___

#if !defined(SHA1_UTILITY_FUNCTIONS) && !defined(SHA1_NO_UTILITY_FUNCTIONS)
#define SHA1_UTILITY_FUNCTIONS
#endif

#include <memory.h> // Needed for memset and memcpy

#ifdef SHA1_UTILITY_FUNCTIONS
#include <stdio.h>  // Needed for file access and sprintf
#include <string.h> // Needed for strcat and strcpy
#endif

#ifdef _MSC_VER
```

```
#include <stdlib.h>
#endif

// You can define the endian mode in your files, without modifying the SHA1
// source files. Just #define SHA1_LITTLE_ENDIAN or #define SHA1_BIG_ENDIAN
// in your files, before including the SHA1.h header file. If you don't
// define anything, the class defaults to little endian.

#if !defined(SHA1_LITTLE_ENDIAN) && !defined(SHA1_BIG_ENDIAN)
#define SHA1_LITTLE_ENDIAN
#endif

// Same here. If you want variable wiping, #define SHA1_WIPE_VARIABLES, if
// not, #define SHA1_NO_WIPE_VARIABLES. If you don't define anything, it
// defaults to wiping.

#if !defined(SHA1_WIPE_VARIABLES) && !defined(SHA1_NO_WIPE_VARIABLES)
#define SHA1_WIPE_VARIABLES
#endif

/////////////////////////////////////////////////////////////////////////////
// Define 8- and 32-bit variables

#ifndef UINT_32

#ifdef _MSC_VER

#define UINT_8  unsigned __int8
#define UINT_32 unsigned __int32

#else

#define UINT_8 unsigned char

#if (ULONG_MAX == 0xFFFFFFFF)
#define UINT_32 unsigned long
#else
#define UINT_32 unsigned int
#endif

#endif
#endif

/////////////////////////////////////////////////////////////////////////////
// Declare SHA1 workspace

typedef union
{
    UINT_8  c[64];
    UINT_32 l[16];
} SHA1_WORKSPACE_BLOCK;

class CSHA1
{
public:
#ifdef SHA1_UTILITY_FUNCTIONS
// Two different formats for ReportHash(...)
enum
{
    REPORT_HEX = 0,
```

```
        REPORT_DIGIT = 1
    };
#endif

    // Constructor and Destructor
    CSHA1();
    ~CSHA1();

    UINT_32 m_state[5];
    UINT_32 m_count[2];
    UINT_32 __reserved1[1];
    UINT_8  m_buffer[64];
    UINT_8  m_digest[20];
    UINT_32 __reserved2[3];

    void Reset();

    // Update the hash value
    void Update(UINT_8 *data, UINT_32 len);
#ifdef SHA1_UTILITY_FUNCTIONS
    bool HashFile(char *szFileName);
#endif

    // Finalize hash and report
    void Final();

    // Report functions: as pre-formatted and raw data
#ifdef SHA1_UTILITY_FUNCTIONS
    void ReportHash(char *szReport, unsigned char uReportType = REPORT_HEX);
#endif
    void GetHash(UINT_8 *puDest);

private:
    // Private SHA-1 transformation
    void Transform(UINT_32 *state, UINT_8 *buffer);

    // Member variables
    UINT_8 m_workspace[64];
    SHA1_WORKSPACE_BLOCK *m_block; // SHA1 pointer to the byte array above
};

//#endif
//#endif // !defined(AFX_SHA1_H__892E0361_14F2_4E6C_85C9_853CF05AC5F8__INCLUDED_)
//{{AFX_INSERT_LOCATION}}
// Microsoft Visual C++ will insert additional declarations immediately before the previous line.

#endif // !defined(AFX_SHA1_H__892E0361_14F2_4E6C_85C9_853CF05AC5F8__INCLUDED_)
#endif // !defined(AFX_SHA1_H__892E0361_14F2_4E6C_85C9_853CF05AC5F8__INCLUDED_)
```

Sha1.cpp .b

```
/*
    100% free public domain implementation of the SHA-1 algorithm
    by Dominik Reichl <dominik.reichl@t-online.de>
    Web: http://www.dominik-reichl.de/

    Version 1.6 - 2005-02-07 (thanks to Howard Kapustein for patches)
    - You can set the endianness in your files, no need to modify the
      header file of the CSHA1 class any more
```

```
- Aligned data support
- Made support/compilation of the utility functions (ReportHash
and HashFile) optional (useful, if bytes count, for example in
embedded environments)

Version 1.5 - 2005-01-01
- 64-bit compiler compatibility added
- Made variable wiping optional (define SHA1_WIPE_VARIABLES)
- Removed unnecessary variable initializations
- ROL32 improvement for the Microsoft compiler (using _rotl)

======== Test Vectors (from FIPS PUB 180-1) ========

SHA1("abc") =
A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D

SHA1("abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq") =
84983E44 1C3BD26E BAAE4AA1 F95129E5 E54670F1

SHA1(A million repetitions of "a") =
34AA973C D4C4DAA4 F61EEB2B DBAD2731 6534016F
*/
#include "stdafx.h"
#include "DigitalSignatureProject.h"
#include "SHA1.h"

#ifdef _DEBUG
#define new DEBUG_NEW
#undef THIS_FILE
static char THIS_FILE[] = __FILE__;
#endif



#ifdef SHA1_UTILITY_FUNCTIONS
#define SHA1_MAX_FILE_BUFFER 8000
#endif

// Rotate x bits to the left
#ifndef ROL32
#ifdef _MSC_VER
#define ROL32(_val32, _nBits) _rotl(_val32, _nBits)
#else
#define ROL32(_val32, _nBits) (((_val32)<<(_nBits))|((_val32)>>(32-(_nBits))))
#endif
#endif

#ifdef SHA1_LITTLE_ENDIAN
#define SHABLK0(i) (m_block->l[i] = \
(ROL32(m_block->l[i],24) & 0xFF00FF00) | (ROL32(m_block->l[i],8) & 0x00FF00FF))
#else
#define SHABLK0(i) (m_block->l[i])
#endif

#define SHABLK(i) (m_block->l[i&15] = ROL32(m_block->l[(i+13)&15] ^ m_block->l[(i+8)&15] \
^ m_block->l[(i+2)&15] ^ m_block->l[i&15],1))

// SHA-1 rounds
#define _R0(v,w,x,y,z,i) { z+=((w&(x^y))^y)+SHABLK0(i)+0x5A827999+ROL32(v,5);
w=ROL32(w,30); }
```

```
#define _R1(v,w,x,y,z,i) { z+=((w&(x^y))^y)+SHABLK(i)+0x5A827999+ROL32(v,5);
                           w=ROL32(w,30); }
#define _R2(v,w,x,y,z,i) { z+=(w^x^y)+SHABLK(i)+0x6ED9EBA1+ROL32(v,5); w=ROL32(w,30); }
#define _R3(v,w,x,y,z,i) { z+=(((w|x)&y)|(w&x))+SHABLK(i)+0x8F1BBCDC+ROL32(v,5);
                           w=ROL32(w,30); }
#define _R4(v,w,x,y,z,i) { z+=(w^x^y)+SHABLK(i)+0xCA62C1D6+ROL32(v,5); w=ROL32(w,30); }

CSHA1::CSHA1()
{
    m_block = (SHA1_WORKSPACE_BLOCK *)m_workspace;

    Reset();
}

CSHA1::~CSHA1()
{
    Reset();
}

void CSHA1::Reset()
{
    // SHA1 initialization constants
    m_state[0] = 0x67452301;
    m_state[1] = 0xEFCDAB89;
    m_state[2] = 0x98BADCFE;
    m_state[3] = 0x10325476;
    m_state[4] = 0xC3D2E1F0;

    m_count[0] = 0;
    m_count[1] = 0;
}

void CSHA1::Transform(UINT_32 *state, UINT_8 *buffer)
{
    // Copy state[] to working vars
    UINT_32 a = state[0], b = state[1], c = state[2], d = state[3], e = state[4];

    memcpy(m_block, buffer, 64);

    // 4 rounds of 20 operations each. Loop unrolled.
    _R0(a,b,c,d,e, 0); _R0(e,a,b,c,d, 1); _R0(d,e,a,b,c, 2); _R0(c,d,e,a,b, 3);
    _R0(b,c,d,e,a, 4); _R0(a,b,c,d,e, 5); _R0(e,a,b,c,d, 6); _R0(d,e,a,b,c, 7);
    _R0(c,d,e,a,b, 8); _R0(b,c,d,e,a, 9); _R0(a,b,c,d,e,10); _R0(e,a,b,c,d,11);
    _R0(d,e,a,b,c,12); _R0(c,d,e,a,b,13); _R0(b,c,d,e,a,14); _R0(a,b,c,d,e,15);
    _R1(e,a,b,c,d,16); _R1(d,e,a,b,c,17); _R1(c,d,e,a,b,18); _R1(b,c,d,e,a,19);
    _R2(a,b,c,d,e,20); _R2(e,a,b,c,d,21); _R2(d,e,a,b,c,22); _R2(c,d,e,a,b,23);
    _R2(b,c,d,e,a,24); _R2(a,b,c,d,e,25); _R2(e,a,b,c,d,26); _R2(d,e,a,b,c,27);
    _R2(c,d,e,a,b,28); _R2(b,c,d,e,a,29); _R2(a,b,c,d,e,30); _R2(e,a,b,c,d,31);
    _R2(d,e,a,b,c,32); _R2(c,d,e,a,b,33); _R2(b,c,d,e,a,34); _R2(a,b,c,d,e,35);
    _R2(e,a,b,c,d,36); _R2(d,e,a,b,c,37); _R2(c,d,e,a,b,38); _R2(b,c,d,e,a,39);
    _R3(a,b,c,d,e,40); _R3(e,a,b,c,d,41); _R3(d,e,a,b,c,42); _R3(c,d,e,a,b,43);
    _R3(b,c,d,e,a,44); _R3(a,b,c,d,e,45); _R3(e,a,b,c,d,46); _R3(d,e,a,b,c,47);
    _R3(c,d,e,a,b,48); _R3(b,c,d,e,a,49); _R3(a,b,c,d,e,50); _R3(e,a,b,c,d,51);
    _R3(d,e,a,b,c,52); _R3(c,d,e,a,b,53); _R3(b,c,d,e,a,54); _R3(a,b,c,d,e,55);
    _R3(e,a,b,c,d,56); _R3(d,e,a,b,c,57); _R3(c,d,e,a,b,58); _R3(b,c,d,e,a,59);
    _R4(a,b,c,d,e,60); _R4(e,a,b,c,d,61); _R4(d,e,a,b,c,62); _R4(c,d,e,a,b,63);
    _R4(b,c,d,e,a,64); _R4(a,b,c,d,e,65); _R4(e,a,b,c,d,66); _R4(d,e,a,b,c,67);
    _R4(c,d,e,a,b,68); _R4(b,c,d,e,a,69); _R4(a,b,c,d,e,70); _R4(e,a,b,c,d,71);
    _R4(d,e,a,b,c,72); _R4(c,d,e,a,b,73); _R4(b,c,d,e,a,74); _R4(a,b,c,d,e,75);
    _R4(e,a,b,c,d,76); _R4(d,e,a,b,c,77); _R4(c,d,e,a,b,78); _R4(b,c,d,e,a,79);
```

```
    // Add the working vars back into state
    state[0] += a;
    state[1] += b;
    state[2] += c;
    state[3] += d;
    state[4] += e;

    // Wipe variables
#ifdef SHA1_WIPE_VARIABLES
    a = b = c = d = e = 0;
#endif
}

// Use this function to hash in binary data and strings
void CSHA1::Update(UINT_8 *data, UINT_32 len)
{
    UINT_32 i, j;

    j = (m_count[0] >> 3) & 63;

if((m_count[0] += len << 3) < (len << 3)) m_count[1]++;

    m_count[1] += (len >> 29);

    if((j + len) > 63)
    {
        i = 64 - j;
        memcpy(&m_buffer[j], data, i);
        Transform(m_state, m_buffer);

for( ; i + 63 < len; i += 64) Transform(m_state, &data[i]);

        j = 0;
    }
    else i = 0;

    memcpy(&m_buffer[j], &data[i], len - i);
}

#ifdef SHA1_UTILITY_FUNCTIONS
    // Hash in file contents
bool CSHA1::HashFile(char *szFileName)
{
    unsigned long ulFileSize, ulRest, ulBlocks;
    unsigned long i;
    UINT_8 uData[SHA1_MAX_FILE_BUFFER];
    FILE *fIn;

    if(szFileName == NULL) return false;

    fIn = fopen(szFileName, "r");
    if(fIn == NULL) return false;

    fseek(fIn, 0, SEEK_END);
    ulFileSize = (unsigned long)ftell(fIn);
    fseek(fIn, 0, SEEK_SET);

    if(ulFileSize != 0)
    {
```

```
            ulBlocks = ulFileSize / SHA1_MAX_FILE_BUFFER;
            ulRest = ulFileSize % SHA1_MAX_FILE_BUFFER;
                }
            else
                {
                ulBlocks = 0;
                ulRest = 0;
                }

            for(i = 0; i < ulBlocks; i++)
                {
                fread(uData, 1, SHA1_MAX_FILE_BUFFER, fIn);
            Update((UINT_8 *)uData, SHA1_MAX_FILE_BUFFER);
                }

            if(ulRest != 0)
                {
                fread(uData, 1, ulRest, fIn);
            Update((UINT_8 *)uData, ulRest);
                }

            fclose(fIn); fIn = NULL;
                return true;
                }
            #endif

            void CSHA1::Final()
                {
                UINT_32 i;
            UINT_8 finalcount[8];

                for(i = 0; i < 8; i++)
            finalcount[i] = (UINT_8)((m_count[((i >= 4) ? 0 : 1)]
        >> ((3 - (i & 3)) * 8) ) & 255); // Endian independent

            Update((UINT_8 *)"\200", 1);

            while ((m_count[0] & 504) != 448)
            Update((UINT_8 *)"\0", 1);

        Update(finalcount, 8); // Cause a SHA1Transform()

            for(i = 0; i < 20; i++)
                {
m_digest[i] = (UINT_8)((m_state[i >> 2] >> ((3 - (i & 3)) * 8) ) & 255);
                }

            // Wipe variables for security reasons
                #ifdef SHA1_WIPE_VARIABLES
                i = 0;
            memset(m_buffer, 0, 64);
            memset(m_state, 0, 20);
            memset(m_count, 0, 8);
            memset(finalcount, 0, 8);
        Transform(m_state, m_buffer);
                #endif
                }

            #ifdef SHA1_UTILITY_FUNCTIONS
        // Get the final hash as a pre-formatted string
```

```
void CSHA1::ReportHash(char *szReport, unsigned char uReportType)
                                                                {
                                                                    unsigned char i;
                                                                   char szTemp[16];

                                                                    if(szReport == NULL) return;

                                                                if(uReportType == REPORT_HEX)
                                                                                {
                                                        sprintf(szTemp, "%02X", m_digest[0]);
                                                                    strcat(szReport, szTemp);

                                                                    for(i = 1; i < 20; i++)
                                                                                {
                                                    sprintf(szTemp, " %02X", m_digest[i]);
                                                                strcat(szReport, szTemp);
                                                                                }
                                                                            }
                                                                else if(uReportType == REPORT_DIGIT)
                                                                                {
                                                                sprintf(szTemp, "%u", m_digest[0]);
                                                                    strcat(szReport, szTemp);

                                                                    for(i = 1; i < 20; i++)
                                                                                {
                                                                sprintf(szTemp, " %u", m_digest[i]);
                                                                strcat(szReport, szTemp);
                                                                                }
                                                                            }
                                                                else strcpy(szReport, "Error: Unknown report type!");
                                                                                }
                                                                            #endif

                                                                    // Get the raw message digest
                                                                void CSHA1::GetHash(UINT_8 *puDest)
                                                                                {
                                                                    memcpy(puDest, m_digest, 20);
                                                                                }
```

- **دالة تكوين الـ Digest**

```
void CDigitalSignatureProjectDlg::OnMakeDigest()
                                                                {
                                                                    char InFile[200];
                                                                   char OutFile[200];

                                                                        UpdateData();
                                                                  strcpy(InFile,m_InputFile);
                                                                 strcpy(OutFile,m_OutputFile);


                                                                    HashFile(InFile,OutFile);
                                                                {
//2- Get the public key of the current user from the database server
                                                                    //search for the user name in the database
                                                                        UpdateData();
                                                                if(ptrDigitalSignatureDB.IsOpen())
                                                              ptrDigitalSignatureDB.Close();
```

```
ptrDigitalSignatureDB.Open(0,"SELECT * FROM Users WHERE
                                        Users.DS_User='"+m_UserName+"'");
                        ptrDigitalSignatureDB.MoveFirst();

                                                }

                                Encrypt("c:\\Temp.txt", m_OutputFile);


                                ptrDigitalSignatureDB.Close();



                                                }
```

- **دالة الإرسال:**

```
                                void CDigitalSignatureProjectDlg::OnPrapare()
                                                {
                                        char InFile[200];

                                                UpdateData();
                                        strcpy(InFile,m_InputFile);


                        //1-Doing Hash Code/////////////////////////////////////////////////
                                        HashFile(InFile,"c:\\TempSource1.hc");

                        //2- combine the original file with the hash code file/////////////////
                        Combine(InFile,"c:\\TempSource1.hc","c:\\TempSource2.cmb");



                        //4- Doing RSA encryption ////////////////////////////////////////////
                        Encrypt("c:\\TempSource2.cmb", "c:\\TempSource2.enc");

                                        //5- Combine the user name and the enc block




                                                char Buffer[200];
                                        strcpy(Buffer,InFile);

                                        Buffer[strlen(InFile)-3]=NULL;
                                                strcat(Buffer,"out");

                                Combine(1,"c:\\TempSource2.enc",Buffer);


                                                }
```

- **دالة الاستقبال**

```
                                void CDigitalSignatureProjectDlg::Oncheck()
                                                {

                                        char InFile[200];

                                                UpdateData();
                                        strcpy(InFile,m_InputReceivingFile);
```

```
//0- seperate the original file and the User Name//////////////////
CString SenderUser;
Seperate(1 ,&SenderUser,InFile ,"c:\\TempDist1.inc");//org=original one


if(MessageBox("Do you want to proceed with a letter comes from:"+SenderUser,"",4)!=6)
return;


//0- Quering from the database/////////////////////////////////////////
QeringForUser(SenderUser);


//1-Decrypt the incomming file ////////////////////////////////////////
Decrypt("c:\\TempDist1.inc","c:\\TempDist1.dec");//dec= decrypted one

//2- seperate the original file and the hash code file//////////////////
Seperate("c:\\TempDist1.dec" ,"c:\\TempDist1.org","c:\\TempDist1.hc");//org=original one

//3- Doing Hashing for original one/////////////////////////////////////////////
HashFile("c:\\TempDist1.org","c:\\TempDist2.hc");

//4- compare the 2 hashing code files
int CheckFlag=Compare("c:\\TempDist2.hc","c:\\TempDist1.hc");


if ( CheckFlag==-1)
MessageBox("File error");
else if (CheckFlag==2)
MessageBox("Not indetical");
else if(CheckFlag==1)
{
MessageBox("OK");
ShellExecute(NULL,"open","c:\\TempDist1.org",NULL,NULL,SW_MAXIMIZE);
}

}
```

- **دالة التشفير**

```
void CDigitalSignatureProjectDlg::Encrypt(CString infile, CString outfile)
{
int NO_BITS=32;
double c=0,d=1;
char bits[100];
double n=(double)m_n;
unsigned char ch;
double data;//19;
long i,k=NO_BITS;
CString str;
int sizeof_d=sizeof(double);


FILE *inFP, *outFP;
inFP=fopen(infile,"r");
```

```
                                        if(inFP==NULL)
                                                {
    str.Format("\nERROR: Couldn't open input file: %s\nAborting operation",infile);
                                                DumpNotes(str);                    //
                                                return;

                                                }

                                        outFP=fopen(outfile,"w");
                                                if(outFP==NULL)
                                                {
str.Format("\nERROR: Couldn't create output file: %s\nAborting operation",outfile);
                                                DumpNotes(str);                    //
                                                fcloseall();
                                                return;

                                                }


                                                //change integer 'm' to binary
                                                        D_to_B(m_e,32,bits);
                                                        GetOnlyProperBits(bits);
                                                k=NO_BITS = strlen(bits)-1;

                                                        while(1)
                                                                {
                                                //read from ip file into 'data'
                                                if(fread(&ch,1,1,inFP)==0)
                                                                break;
                                                        data =(double)ch;

                                //calculate ((data)^e mod n) .i.e the remainder
                                                                c=0;d=1;
                                                        for(i=k;i>=0;i--)
                                                                {
                                                                c=2*c;
                                                        d=fmod(d*d,n);

                                                if(bits[NO_BITS-i] == '1')
                                                                {
                                                        c=c+1;
                                                d=fmod(data*d,n);
                                                                }//end of IF
                                                                }//end of for loop

                                                        //write to op file from 'd'
                                                fwrite(&d,sizeof_d,1,outFP);

                                                                }//end of while loop


                                                                fcloseall();
                                                                }//end of encrypt
```

- **دالة فك التشفير**

```
void CDigitalSignatureProjectDlg::Decrypt(CString infile, CString outfile)
```

```
{
        int NO_BITS;
        double c=0,d=1;
        char bits[100];
    double n=(double)m_n1;
        double data;//19;
            long i,k;
          CString str;
int sizeof_d=sizeof(double);


          FILE *inFP, *outFP;
        inFP=fopen(infile,"r");
            if(inFP==NULL)
                {
str.Format("\nERROR: Couldn't open input file: %s\nAborting operation",infile);
                return;

                }

        outFP=fopen(outfile,"w");
            if(outFP==NULL)
                {
str.Format("\nERROR: Couldn't create output file: %s\nAborting operation",outfile);
                fcloseall();
                return;

                }


            //change integer 'd' to binary
                D_to_B(m_d,32,bits);
            GetOnlyProperBits(bits);
        k=NO_BITS = strlen(bits)-1;

                while(1)
                {
            //read from ip file into 'data'
    if(fread(&data,sizeof_d,1,inFP)==0)
                break;

//calculate ((data)^e mod n) .i.e the remainder
                c=0;d=1;
            for(i=k;i>=0;i--)
                {
                c=2*c;
            d=fmod(d*d,n);

        if(bits[NO_BITS-i] == '1')
                {
            c=c+1;
    d=fmod(data*d,n);
                }//end of IF
                }//end of for loop

            //write to op file from 'd'
     unsigned char ch=(unsigned char)d;
            fprintf(outFP,"%c",ch);
            //write(&ch,1,1,outFP);
```

```
}//end of while loop
fcloseall();
}//end of encrypt
```

Digital Signature Project – Use Case Diagram

igital Signature Project – Use Case Diagram