تقنيات التشفير في التبادل التجاري الالكتروني

م.م. ندى بدر جراح
كلية الادارة والاقتصاد ـ جامعة البصرة

مقدمة :

تعد المعلومات وتقنياتها اهم عناصر البنية الاساسية للتنمية الاقتصادية والاجتماعية في العصر الذي نعيش فيه ، اذ اصبحت المعلوماتية القوة المسيطرة على عناصر الانتاج في مختلف اوجه النشاطات الاقتصادية والمتمثلة في التجارة الإلكترونية او e-Commerce فإلى جانب إمكانية الانترنيت بوضع كميات غير محدودة من المعلومات بين أيدينا، هناك إمكانية شراء المنتجات والخدمات دون مغادرة المنزل، فالتجارة الإلكترونية تعني أنه بمقدورنا القيام بشراء الكتب، والحواسب، وبطاقات السفر، والسيارات، وغيرها في أي لحظة. ومع أن هذه الفكرة كانت مشجعة في بادئ الأمر، إلا أن إنتشارها كان بطيئاً نسبياً بسبب مخاوف العامة، فحفظ المعلومات المصرفية وبيانات بطاقات الائتمان في مكان مجهول يعد مخاطرة كبيرة. ومع أن هذا الخطر محدود، إلا أنه لايزال موجودا".

لهذا الخطر علاقة كبيرة بحقيقة أن معلومات بطاقات الائتمان ترسل ضمن نص غير مشفر، وهذا يعني أنه يمكن سرقة هذه المعطيات واستخدامها بهدف الاحتيال. لقد تم تطوير تقنيات مختلفة للتغلب على هذه المشكلة وحماية المستهلك، مما زرع الثقة في نفوس الناس وشجعهم على الشراء عبر الانترنت.

ومن هذا نجد ان كل فرد او شركة او هيئة تجارية بحاجة للتشفير للحفاظ على خصوصياتها واسرارها ومعلوماتها الهامة جدا"من آن يطلع عليها احد ، فالجميع اليوم لا يستطيع الاستغناء عن خدمات متوفرة في الانترنت مثل البريد الالكتروني وفي المستقبل القريب يكون الجميع بحاجة الى مختلف الخدمات الادارية الإلكترونية كالتعلم والتجارة والبنوك الإلكترونية والمكتبات والخدمات الطبية الإلكترونية ... الخ.

آن رموز التشفير شكلت الاساس لولادة علم التشفير الحديث المستخدم في التجارة الإلكترونية ، اذ آن الكثير من الشركات الكبرى في العالم استفادت اليوم وفي عصر المعلومات هذا من شبكة الإنترنت كبديل لتبادل بياناتها مع شركات اخرى او مع زبائنها ، فقد وفرت شبكة الإنترنت الوسيط الرخيص والواسع الانتشار كي تمارس هذه الشركات تجارة تدر عليها ارباحا" طائلة.

ولقد شهدت اسواق هذه البرامج انتعاشا" مذهلا" بعد آن سمحت السلطات الامريكية للشركات التجارية المتخصصة ببيع هذه التقنية للجمهور وعامة الناس بعدما كانت محصورة للاستخدامات العسكرية والحكومية لسنوات طويلة ، ولقد اتخذت الحكومة الامريكية هذا القرار في سبيل دعم الجانب الامني لمجال التجارة الإلكترونية علما" بانها وحتى وقت قريب لم تسمح بتصدير هذه التكنولوجيا خاصة التي تزيد قوة تشفيرها عن ٥٦ بت .

وان التجارة الإلكترونية تمثل النشاط التجاري لجميع تعاقدات البيع والشراء وطلب الخدمة وتلقيها بآليات تقنية وضمن بيئة تقنية . وضمن هذا المفهوم العام لاحتياجات التجارة الإلكترونية ، تنطوي كافة وسائل ممارسة انشطتها من اجهزة وبرمجيات وحلول وشبكات اتصال ووسائل اتصال وتبادل للبيانات واشتراكات على الشبكة وحلول بشأن امن المعلومات وتنفيذ عمليات الوفاء بالثمن وتقديم الخدمات على الخط . ولان الانترنت، هي شبكة الشبكات ، فقد ارتبط نماء التجارة الإلكترونية ، بل وجودها في وقتنا هذا بشبكة الانترنت.

لقد غيرت الإنترنت وجه عالم التجارة والأعمال،وقد ساهمت شبكات الإنترنت (والإنترانيت والإكسترانت) في تحقيق الوجود الفعلي للتجارة الإلكترونية ، ووفقا للدراسات الإحصائية والتقارير الرسمية وتقارير الجهات الخاصة ، فان نموا كبيرا ومطردا قد تحقق في سوق خدمات الإنترنت والاتجاه نحو التجارة الإلكترونية.

ISSN-1994-697X

ومن الجدير بالذكر ان الشبكة العالمية للإنترنت تتميز بطابع الحرية فهي لا تخضع لهيمنة او هيئة مؤسسة حكومية او غير حكومية حيث لا توجد لها ادارة مركزية محددة ، فضلا" عن ان الإنترنت يشكل مجتمعا" افتراضيا" فضائيا" فهو غير مرتبط بحدود جغرافية ويربط ما يزيد عن ٢٠٠ دولة ويجعلها بحالة اتصال دائم ،وكذلك فان اهم ما تتميز به هذه التقنية هو سهولة الاستعمال وقلة التكاليف وتقديم مختلف الخدمات التعليمية والسياسية والاجتماعية والتجارية والترفيهية وغيرها..

مشكلة البحث :

لتوضيح اكثر الامور التي تبطئ ولوج العراقيين عالم الانترنت عموما" والتعاطي بالتجارة الالكترونية خصوصا" ، يجب ان تعتمد حماية بيانات المتسوقين وبطاقاتهم الائتمانية بتعريف تقنية التشفير لتحقيق درجة مقبولة من الامن والقناعة بخدمة النشاط التجاري الالكتروني وحصول عملية التبادل التجارية عبر الانترنت.

هدف البحث :

تسليط الضوء على جانب تجاري مهم هو سوق المستقبل وامكانية خلق تجارة الكترونية في قطرنا .. ودفع الشركات التجارية والمواطن العراقي الى مزاولة هذه الخدمة بثقة عالية ودون أي تردد بأعتماد طريقة ما تحمي عمليات الاتصال وتضمن حقوق طرفي التبادل وهي عملية التشفير لحماية كل ما يتعلق بنقل المعلومات الحساسة كأرقام الحساب وتحويل الاموال للتسوق عبر الانترنت وبالتالي اعتماد مفاتيح التشفير وفك التشفير واستناد هذه المفاتيح الى صيغ رياضية معقدة ضمن خوارزميات التشفير.

كما ان هدف البحث يكمن في تذليل اهم عقبات التسوق عبر الانترنت وتسريع خطواته من خلال توضيح الطرق الامنة لهذه الخدمة.

فرضيات البحث :

تهيئة بيئة آمنة لخدمة التجارة الالكترونية في العراق وذلك من خلال اخذ اراء عينة من المواطنين والمتمثلين باصحاب الاسواق التجارية والمشتري لمن لهم اتصال واستخدام لشبكة الانترنت باخذ ارائهم في الاجابة على اسئلة تتعلق بمستوى الثقة في التجارة الالكترونية والتداول عبر الانترنت في قطرنا ، ثم التحليل الوصفي لتلك الاجابات والخوض بتلك التجربة التي اجتاحت العالم.

منهجية البحث :

تناول المبحث الاول تعريف مصطلح التشفير بصورة عامة ثم ما يمثل الاستخدام الالكتروني لتلك التقنية في تكنولوجيا التشفير وقوة التشفير ويليه تطبيق تلك التقنية في التجارة الالكترونية باستخدام التوقيع الرقمي والبصمة الالكترونية ، وفي نهاية المبحث لا بد من توضيح عيوب ومساوئ ما ذكر .

اما المبحث الثاني فقد تناول موضوع التجارة الالكترونية واهميتها وموثوقية العمل بها وما المقصود بأمن المعاملات التجارية والعقود الالكترونية.

وفي المبحث الثالث تطرق البحث الى اكثر الخوارزميات استخداما" في تطبيقات الاعمال الالكترونية وهي DES, RSA لانها صممت في اطول اختبار زمني حتى الان ، اضافة الى توضيح نظام تشفير المفتاح العام وامنية RSA.

اما المبحث الرابع فتمثل في الدراسة الميدانية بأعتماد اراء عينة من الافراد ثم بحث الاستنتاجات والتوصيات حول طرح فكرة تفعيل العمل في التجارة الالكترونية بعد توضيح الطرق الآمنة لمزاولتها.

المبحث الأول

اولا: التشفير Cryptography :

هو عملية الحفاظ على سرية المعلومات باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات الى رموز بحيث اذا ما تم الوصول اليها من اشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شئ لان ما يظهر لهم هو خليط من الرموز والارقام والحروف غير المفهومة ، وهي طريقة عملية لحماية المعلومات التي

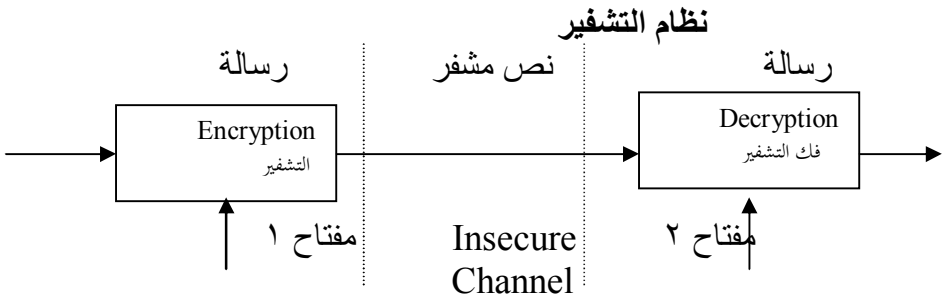
ISSN-1994-697X

تنقل من خلال شبكات الاتصال ، ويمكن استخدامها لغرض صلاحية وسلامة الرسائل و الحماية من مرسل الرسالة الذي ينكر الارسال لاحقا".

ويتم اختيار سلامة انظمة التشفير من خلال اخضاعها الى هجمات تشفيرية .فان هناك عدة معايير (Criteria) التي عادة ما يطلق عليها الهجمات (Attacks) وتستخدم لغرض تحديد ملائمة نظام تشفيري مستقبلي او متوقع ، وفي انظمة التشفير يشفر كل حرف من الكلمة وهناك نوعان شائعان من التشفيرات هما :

(١) التشفيرات الانتقالية حرف النص أي اعادة الترتيب وفق طريقة متفق عليها وهي: الانماط الهندسية ، ابدال السلك ، تغييرات المسلك ، الانتقال العمودي .: وهي عملية تغيير نمط او موقع Transposition Ciphers background

(٢) التشفيرات الاحلالية Substitution Ciphers background : وهي ابدال حروف الرسالة بأرقام متفق عليها أي ابدال رموز برموز اخرى.(٨)



ثانيا" : تكنولوجيا التشفير

هنالك نوعان من التكنولوجيا المستخدمة في التشفير و هي التشفير المتناظر و التشفير غير المتناظر Symmetric Algorithms and Asymmetric Algorithms والفرق بينهم بسيط جدا" ولكنه مهم جدا" في مستوى ودرجة الأمن حيث آن التشفير المتناظر ويستخدم النظام المفتاح ذاته في عمليتي التشفير وفك التشفير. ويعتمد مبدأ هذا النوع على اتفاق الطرفين المرسل والمستقبل للمعلومات المشفرة، على مفتاح سري واحد .ويعتبر عامل أمان هذا النوع أضعف من عامل أمان تشفير المفتاح العام، الذي سيشرح فيما بعد، حيث يمكن أن يتطفل شخص معين على عملية تبادل المعلومات، التي يتم خلالها الاتفاق على المفتاح السري، ويتعرف على هذا المفتاح(١).

اشهر طرق التشفير المتناظر Blowfish , Digital Encryption Standard (DES) , Tiny Encryption Algorithm (TEA), Triple DES , andInternational Data Encryption.

اشهر طرق التشفير الغير متناظر Pretty Good Privacy (PGP) and Reivest , shamir & Aselman (RSA).

وفيما يلي توضيح للمفتاح العام والمفتاح الخاص :

المفتاح العام (Public Key) : هو الرقم الذي يتم تداوله ونشره بين بقية المستخدمين لتشفير أي معلومات او رسالة الكترونية مخصصة لك ويعتبر رقمك العام اساس عملية التشفير ولا يستطيع احد فك رموز تلك المعلومة غيرك انت لانها تحتاج الى الرقم السري وليكن هو المفتاح الخاص بك لاكمال العملية الحسابية والوصول الى الرقم اساسا" وبالتالي فتح الملفات مرة اخرى .

المفتاح الخاص (Private Key) : هو النصف الاخر المكمل للمفتاح العام للوصول الى الرقم الاساس واعادة المعلومات المشفرة الى وضعها الطبيعي قبل التشفير ، وهذا المفتاح هو الذي يميز كل شخص عن غيره من المستخدمين ويكون بمثابة هوية الكترونية تمكن صاحبها من فك أي معلومة مشفرة مرسلة اليه على اساس رقمه العام ولذلك يجب عليك الاحتفاظ بالمفتاح الخاص سرا" وبهذه الطريقة لا يستطيع احد فك الشفرات وقراءة المعلومات المحمية بهذه الطريقة دون اكتمال الحلقة .

ISSN-1994-697X

ثالثاً: قوة التشفير :

تحدد قوة نظام التشفير بناءً على الخوارزمية المتبعة وطول المفتاح المستخدم، ونعني بطول المفتاح: عدد البتات التي يتكون منها المفتاح، ويزداد عامل الأمان كلما زادت. ويمكن أن نشبه مفتاح التشفير، بمفتاح الباب العادي ، فكلما زادت عدد أسنان المفتاح العادي، صعبت عملية تقليده، أو فتح القفل الموافق له .

وتتراوح أطوال المفاتيح المستخدمة في عمليات التشفير ما بين ٤٠ إلى ٢٠٤٨ بت، مع العلم أن المفتاح لا يُعتَبر ذو عامل أمان مرتفع، حسب التقنيات الموجودة الآن، إلا إذا كان طوله يساوي أو يزيد على ١٢٨ بت، حيث تحسب الاحتمالات الممكنة في هذه الحالة من العلاقة (٢ مرفوع للقوة ١٢٨) وتساوي (340,282,366,920,938,463,463,374,607,431,768,211,4 56)احتمال. فإذا أراد شخص أن يخمن المفتاح السري، فعليه أن يجرب هذا العدد من الاحتمالات وبذلك تعتبر قوة التشفير تلك كافية جدا" لحماية التجارة الالكترونية . فان الوقت اللازم لفك شفرة بقوة ١٢٨ بت باستخدام التكنولوجيا الحالية لفك الشفرات هو ٢ ترليون سنة ولذلك لم نسمع ابدا" بان معلومة تم تشفيرها بهذه القوة قد تم فكها من قبل هؤلاء اللصوص المحترفين ونحن لا نعتقد بأن احد يمكنه فعل ذلك على الاقل في المستقبل القريب او المنظور ولذلك تسوق على شبكة الانترنيت وانت مطمئن البال بشرط التأكد من قوة التشفير المستخدمة من قبل الموقع الذي تود التعامل معه وكذلك التأكد من قوة التشفير في متصفحك.

ومن اجل تحقيق تشفير امن لا بد من تلبية العديد من المتطلبات لتقديم العديد من المزايا الامنية وهي كالاتي :

١- يشفر المعلومات ليضمن أن الشخص المقصود بالإرسال هو الوحيد القادر على قراءة هذه المعلومات ، ويدعم أنماطاً متعددة من معايير التشفير

٢- يتحقق من صحة المعلومات ليضمن أن المرسل هو الذي أرسل المعلومات فعلاً، ويتحقق من أن المعلومات لم يتم العبث بها وهي في طريقها إلى الشخص المقصود

٣- يدعم التواقيع الرقمية ليتأكد من هوية المرسل وأنه هو من قام بالإرسال.

٤- يتعامل مع الزبون الذي لا يملك شهادة مفتاح معلن، وهذا يعني أن المستخدم ليس بحاجة إلى تسجيل مفتاح، الأمر الذي يمكن من إنشاء حوار فوري وآمن.

٥- يقوم بتشفير ملف بالكامل أو نموذج صفحة ويب، عوضاً عن تشفير جزء من الملف أو النموذج، وهذا يعني أن نموذج طلب إدخال الأسماء، والعناوين، وأرقام الهاتف، وغيرها من المعطيات ستكون مشفرةً بالكامل على الويب، الأمر الذي يوفر مستوى عالٍ من الأمن(١٣) .

ومن الجدير بالذكر ان استخدام شفرة قوية يعتبر سلاحا" ذا حدين فالاشخاص الملتزمون بالقانون قد يستخدمون شفرة قوية لحماية اسرارهم التجارية وسجلاتهم الشخصية ، الا ان هذه الاسرار يمكن ان تضيع الى الابد اذا فتح مفتاح الشفرة.

رابعاً : التواقيع الرقمية Digital Signature:

التوقيع الإلكتروني عبارة عن جزء صغير مشفر من بيانات يضاف الى رسالة إلكترونية كالبريد الإلكتروني أو العقد الإلكتروني ، وثمة خلط كبير في مفهوم التوقيع الرقمي ، حيث يظن البعض انه أرقام ورموز أو صورة للتوقيع العادي . وهو ليس كذلك ، إذ لا تعد صورة التوقيع العادي بواسطة السكانر (الماسحة الضوئية) توقيعا إلكترونيا.

فالتوقيع الإلكتروني على رسالة ما عبارة عن بيانات مجتزأة من الرسالة ذاتها (جزء صغير من البيانات) يجري تشفيره وإرساله مع الرسالة. بحيث يتم التوثق من صحة الرسالة من الشخص عند فك التشفير وانطباق محتوى التوقيع على الرسالة (١٤) .

ويتم التوقيع الإلكتروني (الرقمي) بواسطة برنامج كمبيوتر خاص لهذه الغاية وباستعماله فان الشخص يكون قد وقع على رسالته تماما كما يوقع ماديا (في عالم الأوراق والوثائق الورقية) ويستخدم التوقيع الرقمي على كافة الرسائل الإلكترونية والعقود الإلكترونية اضافة الى ان الرسالة لم تتعرض لاي تغيير اثناء عملية النقل .

ISSN-1994-697X

إن التوقيع العادي عبارة عن رسم يقوم به الشخص ، انه فن وليس علما ، ومن هنا يسهل تزويره أو تقليده ، أما التوقيع الرقمي ، فهو من حيث الأصل وفي حدود أمن استخدام برنامجه من قبل صاحب البرنامج ، علم وليس فنا ، وبالتالي يصعب تزويره ، وان كان هذا لا يعني انه يمكن عند اختلال معايير الأمن المعلوماتي قد يتم استخدام التوقيع غير الإلكتروني ، وتكمن صعوبة (التزوير) في اختيار أجزاء من الوثيقة المرسلة ذاتها ومن ثم تشفير هذه الأجزاء ، وهو ما يقوم به برنامج الكمبيوتر وليس الشخص ، وتحصين التوقيع الرقمي رهن بحماية سرية كلمة السر ومفتاح التشفير .

وفي بيئة التوقيع العادي على الأوراق أو المحررات ، يمكن اقتطاع الوثيقة عن التوقيع الوارد عنها أو اقتطاع جزء منها واستبداله ، في حين ان ذلك ليس أمرا متاحا في الوثيقة الإلكترونية الموقعة رقميا ، فالتوقيع الرقمي لا يثبت الشخص منظم الوثيقة فقط ، بل يثبت بشكل محدد الوثيقة محل هذا التوقيع ، أنه جزء منها ورموز مقتطعة ومشفرة ، ولدى فك التشفير يتعين أن ينطبق التوقيع ذاته على الوثيقة .

ويرتبط التوقيع الإلكتروني بالتشفير ارتباطا عضويا ، والتشفيرencryption-كما أوضحنا سابقا" هو عملية تغيير في البيانات ، بحيث لا يتمكن من قراءتها سوى الشخص المستقبل وحده ، باستخدام مفتاح فك التشفير . وفي تقنية المفتاح العام يتوفر المفتاح ذاته لدى المرسل والمستقبل ويستخدم في عمليتي التشفير وفك التشفير .

والطريقة الشائعة للتشفير تتمثل بوجود مفتاحين ، المفتاح العام public-key وهو معروف للكافة ، ومفتاح خاص private-key ، يتوفر فقط لدى الشخص الذي أنشأه . ويمكن بهذه الطريقة لأي شخص يملك المفتاح العام ، آن يرسل الرسائل المشفرة ، ولكن لا يستطيع آن يفك شفرة الرسالة . ألا الشخص الذي لديه المفتاح الخاص .

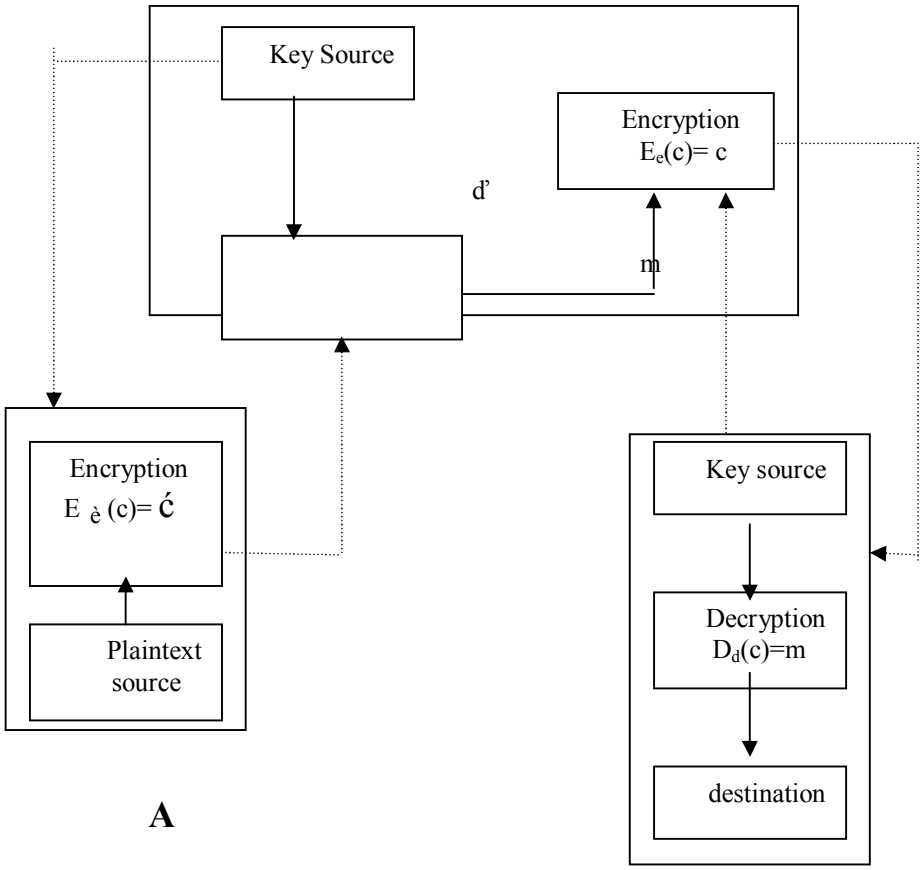
مما تقدم تظهر العلاقة بين التوقيع الرقمي والتشفير ، فالتوقيع الرقمي هو ختم رقمي مشفر ، يملك مفتاحه صاحب الختم . ويعني تطابق المفتاح مع التوقيع الرقمي على الرسالة الإلكترونية آن مرسل الرسالة هو من أرسلها ، فعلا ، وليست مرسلة من قبل شخص آخر كتب عنوانك البريدي لتبدو كأنها مرسلة باسمك . ويضمن التوقيع الرقمي عدم تعرض الرسالة لأي نوع من أنواع التعديل ، بأي طريقة .

ونناقش فيما يلي التواقيع الرقمية النابعة من تشفير المفتاح العام العكسي حيث نفرض آن E_e هو تحويل تشفيري لنظام المفتاح العام وان هناك مساحة عبارة M ومساحة نص مشفر C . نفرض آن M=C فإذا كان D_d هو طريقة تحويل فتح الشفرة المقابل لـ E_e وبما آن كل من D_d ،E_e عبارة عن عمليات تبديل عنصر مكان عنصر فانه يمكن تطبيق ما ياتي : $D_d (E_e(m)) = E_e(D_d(m))=m$

لكل عبارة $m \epsilon M$ آن طريقة تشفير المفتاح العام في هذا النوع يطلق عليه المعكوس(٢) .

ISSN-1994-697X

والمخطط التالي يوضح هجوم انتحال الشخصية في اتصال لمشتركين اثنين :-
هجوم انتحال الشخصية في اتصال لمشتركين اثنين



A

فتسمية التوقيع الرقمي جاءت من كون الرسالة – بعد تطبيق تقنيات التشفير عليها – تظهر بشكل سلسلة من الخانات الرقمية المشفرة (Stream of Digits) وفي نفس الوقت فان تكنولوجيا التوقيع الرقمي (Digital Signature Technology) لها عدة تطبيقات ومنها انها تقدم بديلا" وظيفيا" للتوقيع الخطي التقليدي.

وبذلك فان ظهور واستعمال التوقيع الرقمي في التبادل التجاري الإلكتروني يقصد منه تحقيق ثلاثة أهداف رئيسة هي :

١. موثوقية الرسالة الإلكتروني (Authenticity of Electronic Message) عن طريق ضمان آن الرسالة الإلكتروني قد صدرت من مرسلها الحقيقي (Identification) وتوفير الطمانينة للمستقبل بأن مرسل الرسائل الموقعة لا يستطيع إنكارها.
٢. سلامة الرسالة الإلكتروني من أي تزوير او تعديل (Integrity of E-Message) وذلك عن طريق ضمان آن الرسالة الإلكتروني قد تم تلقيها من المستقبل بنفس المحتوى الذي خرجت به من جهاز المرسل دون آن يتم تعديلها او تغييرها او اضافة أي شيء جديد الى محتواها.
٣. سرية الرسالة الإلكتروني (Confidentiality of E-Message) عن طريق ضمان آن الرسالة الإلكتروني الموقعة بهذه الطريقة لايمكن قراءتها او استيعابها من أي شخص غير مخول ، مما يبعث الراحة والصمأنينة لدى كل من المرسل والمستقبل .

وبذلك يتضح مما سبق آن هناك طرقا" شتى للتوقيع إلكترونيا" على مستند ما وتعرف التوقيعات الإلكترونية التي تعتمد على أساليب التشفير "بالتوقيعات الرقمية" وهذه التوقيعات قد تكون توقيعات تعتمد على ترميز أو تشفير المفتاح العام (الواحد)(Public Key Encryption) أوتشفير المفتاح المزدوج(Public Key and Private Key Encryption) (٦).

ISSN-1994-697X

خامساً: البصمة الالكترونية :

رغم أن التشفير يمنع المتلصِّصين من الاطلاع على محتويات الرسالة، إلا إنه لا يمنع المخرِّبين من العبث بها؛ أي إن التشفير لا يضمن سلامة الرسالة .ومن هنا ظهرت الحاجة إلى البصمة الإلكترونية وهي بصمة رقمية يتم اشتقاقها وفقاً لخوارزميات معيَّنة تُدعى دوالّ أو اقترانات التمويه.

إذ تطبِّق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة . وتُدعى البيانات الناتجة البصمة الإلكترونية للرسالة.وتتكوَّن البصمة الإلكترونية للرسالة من بيانات لها طول ثابت (يتراوح عادة بين 128و١٦٠ بت) تؤخَذ من الرسالة المحوَّلة ذات الطول المتغير. وتستطيع هذه البصمة تمييز الرسالة الأصلية والتعرُّف عليها بدقة، حتى إن أي تغيير في الرسالة - ولو كان في بت واحد- سيفضي إلى بصمة مختلفة تماماً . ومن غير الممكن اشتقاق البصمة الإلكترونية ذاتها من رسالتين مختلفتين. وتتميز البصمات الإلكترونية عن بعضها بحسب المفاتيح الخاصة (private key) التي أنشأتها، ولا يمكن فك شيفرتها إلا باستخدام المفتاح العام (public key)العائد إليها. ولهذا يُطلَق على اقتران التمويه المستخدَم في إنشاء البصمة الإلكترونية اسم آخر هو اقتران التمويه الأحادي الاتجاه .(one-way hash function)(١٣)

ومن الجدير بالذكر، أن استخدام خوارزمية البصمة الإلكترونية أسرع من القيام بعملية التشفير الغير متناظر اي تشفير نص باستخدام المفتاح العام ، ولهذا تُستخدَم خوارزمية البصمة الإلكترونية كثيراً في إنشاء تواقيع رقمية.

سادسا: محاسن ومساوئ تشفير المفتاح العام ازاء تشفير المفتاح السري او الخاص :

آن الفائدة الاساسية من تشفير المفتاح هي زيادة الأمان حيث آن المفاتيح الخاصة تحتاج الى النقل او الكشف الى أي شخص كان و بالمقابل نجد في نظام المفتاح السري بأنه دائما ما تكون هنالك فرصة لامكانية قيام العدو باكتشاف المفتاح السري عند القيام بعملية النقل واما الفائدة الرئيسة الأخرى لانظمة المفتاح العام فهي انها يمكن آن توفر طريقة معينة للتواقيع الرقمية (digital signatures) حيث آن الصلاحية من خلال انظمة المفتاح السري تتطلب المشاركة بسر معين واحيانا تتطلب الثقة من طرف ثالث أيضا اذن فان المرسل يمكن آن ينكر الرسالة الموقعة مسبقا من خلال الادعاء بان السر المشترك قد تمت التسوية عليه من احد الاطراف المشاركة بالسر فعلى سبيل المثال آن نظام كيربروس لصلاحية النتاج السري يشتمل على قاعدة بيانات مركزية تحتفظ بنسخ المفاتيح السرية لكل المستخدمين هذا وان رسالة كيربروس الموثوقة (بالصلاحية) من المحتمل اكثر آن لا تكون ذات ربط قانوني طالما آن الهجوم على قاعدة البيانات سوف يسمح بالتزوير الواسع ومن ناحية اخرى فان صلاحية المفتاح العام تحول دون حدوث هذا النوع من النكران اذ آن لكل مستخدم مسؤولية خاصة به لحماية دوره الخاص .

ويضاف الى ذلك انه يمكن اثبات صلاحية الرسائل الموقعة رقميا الى طرف ثالث كالقاضي مثلا

وهذا يسمح لمثل هذه الرسائل بان تكون مربوطة قانونيا وتجدر الاشارة الى آن انظمة صلاحية المفتاح السري مثل نظام كيربيروس كانت مصممة لتوثيق (لصلاحية) الوصول الى مصادر الشبكة و ليس لصلاحية المستندات (أو الوثائق) وهي مهمة افضل تتحقق به هو من خلال التواقيع الرقمية .

اما المأخذ الذي يمكن باستخدام التشفير بالمفتاح العام فهو السرعة ، حيث توجد هناك طرق تشفير شائعة بالمفتاح السري تكون اسرع بكثير من أي طريقة تشفير متوفرة حاليا" بالمفتاح العام . لكن من خلال هذه الطريقة ستكون لدينا الفوائد التالية(٧) :

١- استخدام اكثر من مفتاح عام وبذلك يكون العدو امام صعوبة اخرى في معرفة أي المفاتيح العامة مستخدمة في التشفير والتي كان سابقا" يعتبرها معلومة جاهزة ولا يفكر في ايجاد الحلول لها. آن هذا الاسلوب يجعل العدو امام اكثر من اختيار وهذا احد عوامل تقوية الامنية.

٢- باستخدام اكثر من مفتاح عام سيكون للمرسل اكثر من مفتاح خاص وهذا يزيد من امنية طرق تشفير المفتاح العام في حالة اكتشاف او ضياع احد المفاتيح الخاصة.

ISSN-1994-697X

٣- التفكير بجدية في تقوية بروتوكول توزيع المفاتيح العامة بسبب تزايد عددها غير آن عدد المشتركين يكون عادة قليلا" في التطبيقات الحساسة وبالتالي لا توجد مشكلة ذات شأن تنجم عن ذلك.
٤- سيكون هناك تغييرا" في مفهوم المفاتيح العامة المستخدمة في طرق تشفير المفتاح العام بحيث يصبح هناك مفتاح خاص مع مفتاح عام سري وليس مفتاحا" عاما" غير سري .

سابعاً: السرية وعيوب التشفير :

من اجل تحقيق السرية الكاملة لاي نظام تشفيري يكون فيه النص الواضح المشفر لا ينتج معلومات ممكنة حول النص الواضح ، وهذا ممكن آن يتحقق نظريا" فقط في حالة ان عدد المفاتيح الممكنة هو على الاقل كبيرا"بعدد العبارات الممكنة ، بمعنى اخر فان المفتاح يجب آن يكون على الاقل بطول العبارة نفسها وعدم تكرار استخدام المفتاح .

كما يستخدم محللو الشفرة الحشو الطبيعية للغة لغرض تقليص عدد النصوص الواضحة الممكنة ، كلما كانت اللغة اكثر تكرارا فانها تكون اسهل لتحليل شفرتها.

ولهذا نجد ان العديد من الاستخدامات التشفيرية في الواقع العملي تستخدم برنامج ضغط لتقليص تكرارية أي عبارة فضلا" عن الجهد المطلوب للتشفير وفك الشفرة.

في النظام التشفيري يعرف مقياس الانتروبي لحجم مساحة المفتاح K كما ياتي(١٠) :

$$H(k)= \log_2 k$$

ولا بد آن نذكر فيما ياتي عيوب التشفير للتوضيح واخذها في نظر الاعتبار رغم ما يتم غالبا" التغاضي عنها :
١- التشفير المكسور للخدمات المجهولة تجعل الوثائق ضد الاعتراضات القانونية .
٢- استخدام التشفير من العملاء والخونة حيث تكون المعاملات الإلكتروني بعيدة عن أي تنظيم حكومي او مراقبة .
٣- التشفير طريقة لتهديد المنظمات والاشخاص في حالة بيع معلومات الكترونية من موظف في الشركة الى منافس ما بدون استنساخ أي وثيقة .
٤- ارتفاع قيمة الوسائل التقنية للحماية تضاف الى كلفة البرنامج اصلا"، ويدفع هذا الامر بمقتني البرامج الى اقتناء برامج اقل تكلفة والتي ستكون ايسر اختراقا".

المبحث الثاني

اولا" : التجارة الإلكترونية Electronic Commerce

تمثل التجارة الإلكترونية واحدا من موضوعي ما يعرف بالاقتصاد الرقمي Digital Economy حيث يقوم الاقتصاد الرقمي على حقيقتين :- التجارة الإلكترونية و تقنية المعلومات Information Technology- IT فتقنية المعلومات او صناعة المعلومات في عصر الحوسبة والاتصال هي التي خلقت الوجود الواقعي والحقيقي للتجارة الإلكترونية باعتبارها تعتمد على الحوسبة والاتصال ومختلف الوسائل التقنية للتنفيذ وادارة النشاط التجاري .

فالتجارة الإلكترونية هي تعامل تجاري مثل ذلك التعامل التجاري الذي يجري على الارض غير آن ابرام العقد والدفع فيه يتم بصورة الية الكترونية غير مباشرة ، فهي تجارة تجري احداثها بين مستعمل للحاسب ومستعمل اخر كلاهما متصلان على شبكة الانترنيت او بين مستعمل للحاسب والحاسب المربوط على الشبكة العالمية للاتصالات.

إن الصفة العالمية للتجارة الإلكترونية ألغت الحدود والقيود أمام دخول الأسواق التجارية ، وبفضلها تحول العالم إلى سوق مفتوح أمام المستهلك بغض النظر عن الموقع الجغرافي للبائع او المشتري (٤) .

والتجارة الإلكترونية (E-commerce) هي تنفيذ و إدارة الأنشطة التجارية المتعلقة بالبضاعة والخدمات بواسطة تحويل المعطيات عبر شبكة الإنترنت أو الأنظمة التقنية الشبيهة ، وتنطوي على عناصر وتثير تحديات في سائر الحقول والموضوعات المشار اليها وهي امن المعلومات ووسائل الدفع الالكتروني والملكية الفكرية والتعاقد الالكتروني والحجية والمعايير و... الخ

ISSN-1994-697X

وهنا لا بد آن نذكر التحديات في حقل بناء تجارة الكترونية عربية او عراقية :-

الاول : متطلبات البنى التحتية ، وهو تحد ذو طبيعة تقنية تتصل به تحديات بناء وتطوير الكوادر البشرية في حقل المعرفة التقنية وتحديات استراتيجيات وهي ادارة مشاريع المعلوماتية في القطاعين العام والخاص وسلامة التعامل مع لغتها ومتطلباتها .

الثاني : فيتمثل بتحديات البناء القانوني الفاعل المتوائم مع واقع المجتمع والامة والمدرك لابعاد التأثير على ما هو قائم من مرتكزات وقواعد النظام القانوني ، وهو تحد ذو طبيعة تنظيمية .

الثالث: فيتمثل بتحديات التميز والاستمرارية والقدرة التنافسية ، وهو تحد يتصل بالاعمال او على نحو ادق بمفهوم تطوير الاعمال .

ويشتمل نطاق التجارة الالكترونيةعلى اعمال كثيرة مثل نظام تبادل المعلومات الالكتروني او التبادل الالكتروني للبيانات (EdI ، Electronic Data Interchange) والتحولات المالية الإلكتروني (Electronic Fund Transfer , EFT) كما ويشتمل ايضا" على استعمال المواقع على شبكة الانترنيت (الويب) للمخاطبة والاتصال بالمستهلكين والمتسوقين ، وبأختصار فأن التجارة الإلكتروني تستخدم مجموعة من المعطيات أهمها :

١. نظام تبادل البيانات والمعلومات الإلكترونية (EDI) ، والذي يعتبر اول صور التجارة الإلكترونية ظهورا" واستعمالا" .
٢. البريد الالكتروني (E-mail) والذي انتشر وتوسع التعامل به لاحقا" نتيجة تطور شبكة الانترنيت واستخداماتها.
٣. لوحات الحاسوب الاعلانية الإلكترونية (computerBulletin ,boards)
٤. وتقنيات اخرى يأتي في مقدمتها شبكة الانترنيت كنظام قائم متكامل والتي تعتبر صاحبة الفضل في ازدهار التجارة الإلكترونية وانتشارها ، اذ لايمكن التحديث عن التجارة الإلكترونية بمفهومها العالمي كوسيلة حديثة من وسائل اتمام العمليات والصفقات التجارية والمحلية والعالمية على حد سواء في غياب شبكة الانترنيت.

ثانيا" : اهمية التجارة الإلكترونية

تكمن اهمية التجارة الإلكترونية في كونها مؤهلة لتصبح ركيزة التجارة الدولية نتيجة لاعتمادها على شبكة الانترنيت العالمية واسعة الانتشار والتي أظهرت نوعا" جديدا" ومستحدثا" للتبادل التجاري بين البائعين والمشترين من مختلف دول العالم ، والذين وجدوا في التجارة الإلكترونية عبر الانترنيت وسيلة سهلة ورخيصة للانتشار والتسوق على مستوى العالم ، فلا يحتاج البائع او التاجر أرسلها لمجرد اتخاذ موقع له على شبكة الانترنيت (World Wide Website) او انشاء عنوان بريد الكتروني (E-Mail) لكي تفتح امامه افاق جديدة من المعرفة والتجارة وليصبح على اتصال بالعملاء والمتسوقين في مناطق كان يتعذر الوصول اليها من قبل أرسلها بصعوبة وتكلفة مرتفعة ، وفي المقابل فقد فتحت التجارة الإلكترونية المجال امام المستثمرين والمتسوقين للتعامل مع البائعين في الاسواق المحلية و العالمية بضغطة واحدة على جهاز الحاسب (AMouse Click) لطلب السلعة او الخدمة التي يرغب في الحصول عليها ودون الحاجة الى الدخول في علاقة مباشرة مع البائع الامر الذي يميز التجارة الإلكتروني عن التجارة التقليدية من حيث آن البائع و المشتري يظلان حكما على اتصال دائم بينهما في مجلس العقد على الرغم من تباعد المكان و الموقع بينهما .

هذا التطور المطرد يجعل في حكم المؤكد آن تطبيق اساليب التجارة الإلكترونية في العلاقات التجارية بين الدول امر لن يكون اختياريا" يتم الاخذ به او تركه بل انه اصبح حقيقة عالمية واقعة من حقائق الحياة التجارية لا يمكن التخلف عنها.

وبالاضافة لما سبق ذكره يمكن اجمال المنافع المتاتية من دخول انظمة التبادل الالكتروني للبيانات و التجارة الإلكترونية للحياة التجارية للافراد و الشركات و في المراسلات و المعاملات الحكومية بما يلي(٩) :

١. آن الاسلوب غير التقليدي للتجارة الإلكترونية في الوصول الى المشتري في كافة انحاء العالم يؤدي الى تحقيق عائدات ضخمة يقابلها انخفاض كبير في تكاليفها مقارنة بالاساليب التقليدية ، فالتجارة الإلكترونية تزيد فرص التسويق للشركات البائعة و تزيد من خيارات المشترين والمتسوقين في آن واحد .

ISSN-1994-697X

٢. يمكن من خلال التجارة الإلكترونية تحسين جودة و نوعية العمل و ادارة الشركات و المؤسسات لعملياتها بشكل اكثر فعالية ودقة يخفض من الوقت المطلوب لمعالجة المعلومات و يقلل من مخاطر التفسير الانساني الارتجالي للمعلومات و البيانات كما و يقضي على الوقت الضائع في العمل المؤسسي .
٣. زيادة عدد و كمية و دوران الفرص التجارية بين الشركات من جهة وفيما بين الشركات و الحكومات من جهة اخرى ، مما يؤدي الى انتشار اوسع للمعلومات المتعلقة بالمشتريات و عطاءات التوريد على كافة الاصعدة الخاصة و العامة ، كما توفر التجارة الإلكترونية معلومات يومية عن الزبائن و هذا بلا شك يؤدي الى خفض تكلفة المعاملات التجارية لانها تلغي دور الوسطاء بين البائع والمشتري.
٤. التقليل من مخاطر الموجودات والمخزون ، فبأستخدام التجارة الإلكترونية تستطيع الشركات معالجة الطلبيات والوفاء بها بكفاءة زمنية وفنية عالية من خلال اتباع اساليب جديدة وسريعة لادارة المخزون والسلع والبضائع باستخدام أنظمة التبادل الالكتروني للبيانات .
٥. تخفيض الاجور الكلية للمراسلات البريدية والقضاء على ظاهرة فقدان الرسائل البريدية وفي القطاع العام وتسريع المراسلات وتبادل المعلومات بين الدوائر الحكومية المختلفة.
٦. تخفيض الوقت المطلوب للاستلام والاجابة على الطلبيات واوامر الشراء وتسريع عملية ارسال اوامر الدفع والفواتير قيد التحصيل وانتشار اساليب جديدة للتحصيل وارسال الفواتير.
٧. امكانية اجراء المخاطبة الفورية المباشرة بالصوت والصورة بلا حواجز ولا قيود الامر الذي يؤدي الى زيادة احجام التجارة الدولية.
٨. تشكل التجارة الإلكتروني – كعصب حيوي في عمليات التجارة الحرة – حجر زاوية في تأسيس اليات التنسيق الاقتصادي الاقليمي وخصوصا" التنسيق الاقتصادي العربي ، حيث يجب آن لا يستغرق عملية انتقال المعلومات من بلد عربي الى اخر سوى ثوان معدودة او المعكوس منها، وهذا بدوره يشكل فرصة يجب انتهازها لانشاء سوق عربية مشتركة تكون مشاركتها عالية في مردود التجارة العالمية (٣) .

ثالثا" : موثوقية التجارة الإلكترونية

ان سعي الهيئات والجهات التي تتبنى نشاطا" معلوماتيا" لتسيير حركتها في الحفاظ على معلوماتها واسرارها وتخزينها بعيدا" عن ايدي محترفي الجريمة المعلوماتية يظهر بشكل جلي وواضح في مجال التجارة الالكترونية ومنها التعاقد بالانترنت.

فمما لا شك فيه ان التجارة الالكترونية التي شاع استخدامها قد اوجدت من الوسائل الفنية التي تمكن البائع والمشتري من ان يطمئنا الى وفاء التزام كل منهما قبل الاخر وعدم تسرب البضاعة وذهابها الى غير مشتري وعدم تسرب وذهاب الثمن الى غير البائع الى جانب عدم افشاء كل ما يتعلق بأسرار كل منهما سواء بكشف اسرار حساب او الرقم السري لحساب أي منهما ، ويتم هذا عن طريق استخدام طريقين اساسيين هما(٥) :-

- التحقق من شخصية المتعاقدين
- استخدام اسلوب التشفير

ويتم التحقق من شخصية المتعاقد عن طريق استخدام شفرة المفتاح العام Publick Key من قبل الطرفين المتعاقدين بان يوقعا على المستندات بطريقة رقمية وبالتالي يصعب انكار الرسالة المرسلة او العقد المبرم بينهما وذلك لان مستقبل الرسالة هو الوحيد الذي يعرف المفتاح الخاص لمرسل الرسالة والذي يمكنه وحده فقط قراءتها، بحيث انه لو وجد احد المفتاحين عند احد ما قد استطاع الحصول عليه فأنه من الصعب عليه تخمين المفتاح الاخر.

عندما يشرع مستخدم ما على موقع بانشطة التجارة الإلكترونية على الخط ، يبدأ بطلب السلعة او المنتج او الخدمة ، وبالنسبة للقائم على موقع التجارة الإلكترونية ، فان المهم لديه التوثق من صحة الطلب ، ويتطلب ذلك ابتداء التوثق من آن من يخاطبه هو فعلا من دون اسمه او عنوان بريده الالكتروني او غير ذلك من معلومات تطلبها مواقع التجارة الإلكترونية ، فكيف يتم ذلك ، خاصة في ظل تنامي اجراءات الاختراق واساءة استخدام اسماء الغير في انشطة جرمية على الشبكة وبنفس الوقت سيجيب موقع التجارة الإلكتروني

الطلب وتحديدا الالتزام بتسليم محل التعاقد ، فما الذي يضمن للمستخدم آن ما وصله من معلومة انما جاءته من هذا الموقع وما الذي يضمن له ايضا آن هذا الموقع حقيقي وموجود على الشبكة ، وحل هذه المعضلة تحتاج ايجاد حلول تقنية (كوسائل التعريف الشخصية عبر كلمات السر والارقام السرية ، او وسيلة التشفير عبر ما عرف بوسيلة المفتاح العام والمفتاح الخاص ، ووسائل التعريف البيولوجية للمستخدم كبصمات الاصابع المنقولة رقميا او تناظريا وسمات الصوت او حدقة العين او غيرها) ، وهي وسائل اريد منها ضمان تأكيد الاتصال واثبات صحة صدور المعلومة عن النظام التقني الصادرة عنه ، لكن لكل منها ثغراته الامنية التي غالبا"ما تكون غير كافية ومن هنا لا بد من اللجوء لفكرة الشخص الوسيط في العلاقة ، وهو جهة تؤكد صحة التعامل على الخط ، وهي شركات ناشطة في ميدان خدمات التقنية تقدم شهادات تتضمن تأكيدا آن الطلب او الجواب قد صدر عن الموقع المعني وتحدد تاريخ ووقت صدور الطلب او الجواب ، وحتى تضمن شخصية المخاطب توفرت تقنيات التعريف على الشخص ، بدأ بكلمة السر وانتهاء بالبصمة الصوتية ، فضلا" عن تقنيات التشفير التي يزداد الجدل حول مشروعيتها ، وذلك في ظل اثرها المانع والمقيد لحرية تدفق البيانات وانسيابها ومساسها في كثير من الحالات بالخصوصية سيما عند اجراء عملية التوثق وتفتيش النظم .

وقد اثير في ميدان العلاقات القانونية للتجارة الإلكترونية ، مسألة مسؤولية الشخص الثالث ، وتحديدا مزودي خدمات الانترنت ، وجهات استضافة المواقع او الجهات المناط بها تسجيل الموقع ، هل تسأل عن انشطة المواقع التي تحتال عبر الايهام بوجود نشاط تجاري الكتروني ، سواء اكان غير قائم او غير محقق لما يعلن عنه ،، وتتجه التشريعات نحو ابراء الشخص الثالث من هذه المسؤوليات بكونه غريبا عن العلاقة العقدية ولتوفر وسائل الأمن التقنية وشركات تعطي اطراف العلاقة قدرة على ضمان حقوقهم بعيدا عن الشركات المزودة للخدمات التقنية .

أما عن مسؤولية الشركات المتعاقد معها لضمان اثبات شخصية الطرف الاخر وصحة الاتصال ، فان الاتجاه الغالب يذهب الى مسؤوليتها عند ايرادها معلومات خاطئة او غير دقيقة ، باعتبار آن التعاقد انبنى على هذه المعلومات وسندا لوجود التزام قانوني عليها ، في الغالب يكون لقاء ما يدفعه الزبون لها لضمان صحة تعاملاته التجارية على الخط .

رابعا" : أمن المعاملات التجارية والعقود الإلكترونية :

على الرغم من ان تحويلات التبادل الالكتروني على درجة عالية من الامان .. الا ان العموم لا يزال على درجة عالية من الخوف من استخدام بطاقات الائتمان للدفع عبر الشبكة ، ولحل هذه المشكلة نجد رجال التسويق يستخدمون الخوارزميات المشفرة ويعيدون التأكيد على المستخدمين في كل مرحلة من مراحل الشراء على امن العملية.

تتطلب عمليات التجارة الالكترونية الكبيرة على الشبكة برمجيات واجهزة باهضة التكلفة ، خاصة" اذا كانت تستخدم تطبيقات تجميع وتوزيع البيانات بشكل كثيف حيث تظهر تكنولوجيا جديدة لزيادة درجة الامان على الإنترنت وادوات ووسائل دفع جديدة مثل البطاقات الائتمانية الخاصة بالشراء من المواقع الالكترونية فقط ، فيجب على المؤسسات ان تعطي اهتماما" خاصا" للتكنولوجيا للاستراتيجات التجارية اذا ارادت ان تحقق النجاح باستخدام نموذجا تجاريا قابلا للتطبيق والنمو سواءا كان ذلك على شبكة الإنترنت او خارجها(١٢) .

وفيما يتعلق بأمن الشبكة فان الشبكات الخاصة الافتراضية التي تعتبر شبكة الانترنت شبكة عامة تقوم بتوثيق وتشفير البيانات قبل تبادلها. او استخدام نظم التشفير ، مع مراعاة المشكلات القانونية المتصلة بها وقيود التصدير ، والتشفير عنوان وسائل امن التقنية في الوقت الحاضر .

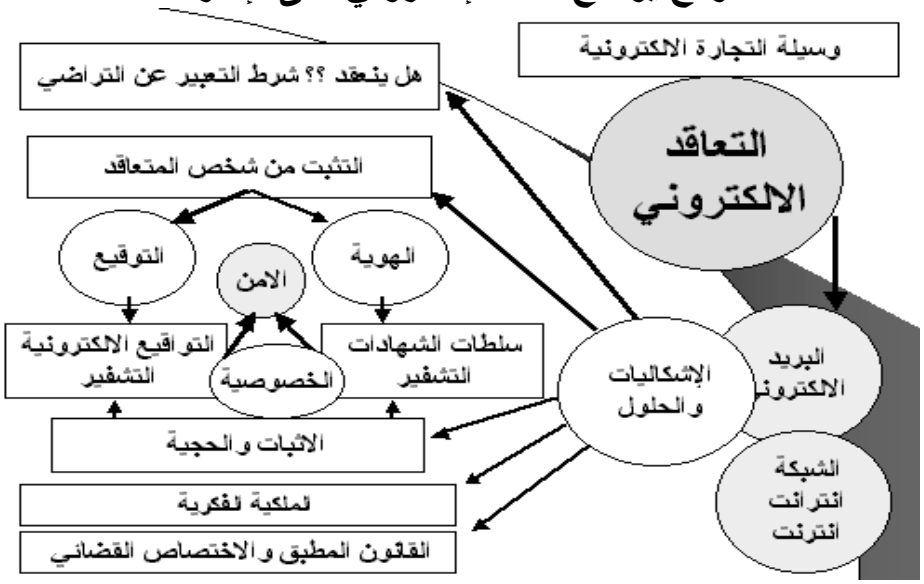
وان هذه الطريقة في حقيقتها طريقة مقنعة للتعاقد ، لكنها لم تكن يوما طريقة واضحة ، ولم تكن تشعر أن العقد ملزم ، لان أحدا لم يكن يهتم لقراءة الرخصة وكان الأساس التاريخي والعملي لعقود الويب أو العقود الإلكترونية ويستخدم العقد الالكتروني لكافة التصرفات محل الاتفاقات على الشبكة ، وبشكل رئيس :- انزال البرامج او الملفات عن الشبكة ، الدخول الى خدمات الموقع وتحديدا التي تتطلب اشتراكا خاصا في بعض الاحيان او مقابل مالي او لغايات الحصول على الخدمة (كالمحادثة ومجموعات الاخبار او الاعلان والادلة) او لغايات التسجيل والالتزام العقدي بانفاذ الخدمة المعروضة مجانا بشروط الموقع كخدمات البريد المجاني

ISSN-1994-697X

والاستضافة المجانية وغيرها.وكذلك لابرام التصرفات القانونية على الخط كالبيع والشراء والاستئجار وطلب القرض واجراء عملية حوالة مصرفية وابرام بوالص التأمين ودفع الثمن وغيرها .

ومن حيث أهمية العقد الإلكتروني ، فان تقنية العقود الإلكترونية توفر قدرة التعاقد على الشبكة وفي بيئتها والحصول على الخدمات والبضائع والمصنفات بارخص الاسعار ومن خلال قوائم اختيار معروفة وواسعة ومن أي موقع او مصدر للموردين على الخط ، كما تتيح للمورد تحديد التزاماته بوضوح وتحديد نطاق المسؤولية عن الخطا والاضرار جراء التعاقد او بسبب محل التعاقد كأخطاء البرمجيات ومشاكلها ، وتساهم في تسهيل المقاضاة بين الطرفين لما تقرره من قواعد شاملة بالنسبة للحقوق والالتزامات(٣) .

نموذج يوضح العقد الإلكتروني على الإنترنت



المبحث الثالث

اولا: **خوارزمية** RSA

ان خوارزميات التشفير مصممة لحماية المعلومات اثناء عملية انتقالها فعن طريقة التشفير المعروفة باسم RSA لم يتم كسرها الا في مختبرات الجامعات وذلك بأستخدام كمبيوترات عالية السرعة واسابيع متواصلة من العمل وبالتالي فأن معلومات المستخدم تعتبر أمنية جدا" اثناء عملية النقل .

متصفح المستخدم يقوم بتشفير رقم بطاقة الائتمان ثم يرسلها الى البائع ، البائع يقوم بدوره بتشفير المعلومات الخصوصية ويعيدها للمستخدم وان لكل موقع مفتاح لفك تشفير الرسائل ولكن يجب ان يحصل المستخدم على مفتاح البائع وهذا ما هو معروف بالمفتاح العام ومن الجدير بالذكر هو ان خوارزميات التشفير ذكية جدا" حيث نجد ان المفتاح العام يستطيع تشفير الرسائل لكنه لا يستطيع فك تشفيرها الا المفتاح الخاص والذي يحتفظ به البائع.

البرنامج الذي يتولى عملية التشفير هو جزء من الخادم الخاص بالبائع ، قفل صغير على نافذة المتصفح يؤشر على عملية اتصال مشفرة مع البائع ، تصميم هذا القفل يمكن ان يكون قد تسبب في تحديد نمو التجارة الالكترونية ،وبهذا نجد ان المستهلك يكون متأكد ومطمئن اكثر للعملية ، فالتشفير يحمي المعلومات اثناء عملية النقل بين المستخدم والبائع.

ثانيا" : **نظام تشفير المفتاح العام** RSA

لقد سمي نظام التشفير RSA بهذا الاسم نسبة الى مكتشفيها رايفست وشامير وادلمان وتم اكتشافها في العام ١٩٧٠ وتعتبر من اكثر طرق التشفير في انظمة المفتاح العام وان RSA هو نظام يوفر كل من الامنية

والتواقيع الرقمية باعتمادها على التعقيد لمسألة تحليل عوامل الاعداد الصحيحة. وان هذا النظام يعمل كما ياتي(٨) :

(١) خذ عددين اوليين p وq وجد ناتجهما كآلاتي :

$$N = p * q$$

حيث آن q,p,n تدعى باسم التركيبات (modules).

(٢) اختر عدد صحيح عشوائي e والذي يعتبر المفتاح العام اقل من ومساويا" نسبيا" لـ

$$Ø(n) = (p -1)*(q -1)$$

(Ø Euler function) وجد معكوس هذه الدالة ed أي :

$$ed = 1(\text{mod } Ø(n))$$

(٣) يتم جعل الزوج (n,e) عاما" او علنيا" في حين يتم الابقاء على d سرية وكذلك يجب الابقاء على سرية العاملين p وq.

(٤) يمكن تحقيق التشفير عن طريق استخدام المفتاح العام كـ:

$$C = M^e \ (\text{mod } n)$$

(٥) يمكن تحقيق فك التشفير عن طريق استخدام المفتاح الخاص كـ:

$$M = C^d \ (\text{mod } n)$$

نلاحظ انه في اكثر طرق تشفير المفتاح العام آن هناك مفتاحان احدهما معلن وهو المفتاح العام والاخر سري وهو المفتاح الخاص ومن المسائل المهمة لتقوية امنية المفتاح العام هو ضرورة آن يمتلك هذا المفتاح نوعا" من السرية ليزيد بذلك من الصعوبات التي تواجه محللي الشفرة والتي تعتمد في الاساس على البحث عن تحليل العوامل مثلا" في طريقة RSA لاكتشاف المفتاح الخاص ولا يفكر في المفتاح العام.

آن احد الوسائل التي يمكن آن تعطي نوعا" من الانتباه لمحلل الشفرة هي ان يجد امامه صعوبة اخرى من ناحية المفتاح العام ، وان هذه الوسيلة تكون بأن يختار المرسل اكثر من مفتاح عام يفي بالشرط.

فان امن المكون الخاص في نظام RSA يعتمد على صعوبة تحليل الاعداد الصحيحة الكبيرة الى عواملها . ولا تعرف اية خوارزمية كفوءة لهذه المشكلة عند برهنتها لتكون (NP- complete). هذا وان صعوبة احتساب اللوغارتمات المنفصلة تحرف هجمات النصوص الصريحة المعلومة، حيث يتوجب استخدام تركيبة لوغارتم منفصل اذا ما اردنا ايجاد d من

$$C = M^e \ (\text{mod } n)$$

وفي نظام RSA وعندما يتم استخدامه كخطة للتوقيع الرقمي ، تكون خاصية المضاعفة كما ياتي : $S_1 = M_1^d (\text{mod } n)$ و $S_2 = M_2^d (\text{mod } n)$ ، حيث آن d هي المفتاح الخاص ، ونستطيع تزوير رسالة صحيحة اخرى وزوج من التواقيع : $\{(S_1 * S_2), (M_1 * M_2)\}$ كما انه من خلال معرفة التوقيع S للرسالة M يمكننا احتساب التواقيع M^{-1} وM- كما ياتي :

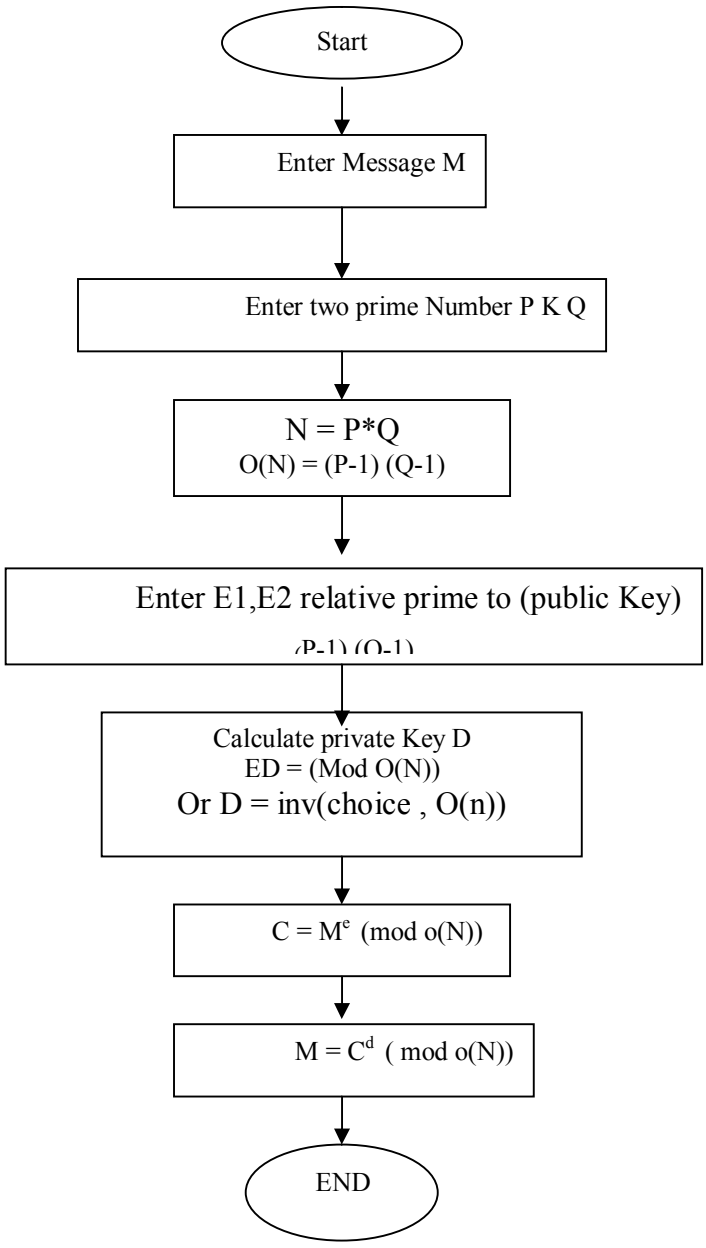
$$S = (M^d)^{-1} = (M^{-1})^d \ (\text{mod } n) \text{ and } -S = (-M)^d = -1^d * M^d * -M^d (\text{mod } n)$$

(while d is odd)

آن هجوم النص الصريح المعلوم هذا يمكن توسيعه الى هجوم النص الصريح المختار وهجوم النص الصريح المختار التكيفي والذي يمكن انجازه من دون معرفة d. كما آن هذا الهجوم يقود الى اعداد جدول بازواج الرسائل والتواقيع ، ومن خلال استخدام هذا الجدول نستطيع تقسيم الرسالة المقصودة الى ناتج رسالة معينة في الجدول ونقوم بشكل ناجح بتزوير التوقيع السليم المرغوب من خلال ناتج التوقيع المتلازم المدخر في الجدول ، هذا وان خاصية المضاعفة تجعل من هذا الهجوم يعمل بشكل فاعل.

ISSN-1994-697X

مخطط انسيابي لالية تقوية امنية البيانات في اخفاء وتبديل المفتاح العام في RSA

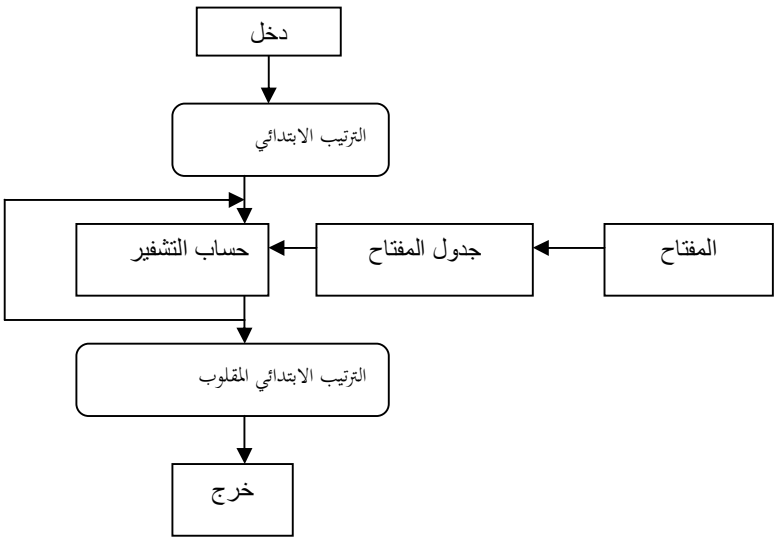


ثالثا" : **خوارزمية الـ**DES :

وهنا لابد ان نوضح بشكل مختصر شيئا" عن خوارزمية التشفير الـ DES لاجل المقارنة ليس الا.. فهي خوارزمية تشفير البيانات Data Encryption Algorithm وهي طريقة الخطوة – بعد – الخطوة لحل المشكلة ، وان المشكلة التي تتعامل معها تتضمن تشفيرا" وفك شفرة مقاطع من البيانات مكون كل منها من ٦٤بتا" طولا" ، والدواخل هي ٦٤بتا" ، والخوارج هي ٦٤بتا" ، والمفتاح المستخدم في العملية هو ايضا" بطول ٦٤بتا" وان الـDES يعامل ال٦٤بتا" من الدواخل في ما يدعى بالشفرة الكسرية المدورة ، وان ابتداء وانتهاء الـDES هو عبارة عن ترتيب أولي وترتيب اولي معكوس على التعاقب كما في الشكل التالي :-

ISSN-1994-697X

خوارزمية الـDES



ومن ميزات الـDES بانها سريعة وبالإمكان بناءها على شكل دوائر كهربائية وذلك لانها لا تحتوي على عمليات رياضية كما ان لها امنية عالية وفي الاتجاه الاخر نجد ان من مساوئها هو انها تعاني من مشكلة توزيع المفاتيح.

رابعا" : **أمنية الـ** RSA :

لم يبرهن استحالة فتح شفرة العبارات المشفرة باستخدام نظام التشفير RSA بدون تحليل عوامل n ، لكن لم يتم اكتشاف ذلك حتى الان ، وذلك لان عملية تحليل عوامل اعداد صحيحة كبيرة مشكلة معقدة الحل وتحتاج الى وقت طويل في الحاسبة ، ومن هنا نجد ان RSA تكون معرضة للانتهاك عندما يصبح تحليل عوامل N ممكنا". ولتلافي هذا تستخدم الاعداد الاولية P ، Q ولكل واحد منهما عدة مئات من الخانات الرقمية، لغرض حماية امنية العبارات لعشرات او مئات السنين .

فضلا" عن ان مشكلة حساب اس التشفير (d) للـRSA من المفتاح العام (n,e) هما حسابيا" متكافئتين، وعند توليد مفتاح الـRSA فأن من الامور الاساسية والضرورية انه يتم اختيار الاعداد الاولية q,p بطريقة معينة بحيث ان تحليل n الى عواملها (n=pq) يكون حسابيا" متعذر التنفيذ (١١).

ولا يوجد شئ يمنع محلل الشفرة من تجريب كل الطرق الكلاسيكية ضد RSA ومن نقاط الضعف :

- الهجوم بواسطة تحليل العوامل
- الهجوم باستخدام التكرار
- الهجوم في حالة قيمة صغيرة لـe.
- الـRSA تحتاج نسبيا" الى مفتاح طويل وفي المستقبل القريب يكون الطول ١٠٢٤بت او اكثر وان زيادة طول المفتاح المستخدم يزيد الامنية وتقل السرعة ويمكن تجاوز هذا الضعف باستخدام الحاسبات المتوازية.
- الـRSA بطيئة مقارنة بخوارزميات التشفير الاخرى، فهي ابطأ من خوارزمية الـDES بحوالي ١٠٠٠مرة ، وقد ظهر العكس في دراسات متعمقة اخرى.
- فقدان المفتاح السري ولذلك فعلى المستفيد الاحتفاظ بنسخة اخرى منه.

ISSN-1994-697X

المبحث الرابع

اولا" : الدراسة الميدانية :

ولتوضيح امكانية تطبيق التجارة الالكترونية في العراق وتوسيع هذه الخدمة تحت بيئة اتصالات آمنة ، تم اعداد استمارة استبيان تحتوي على مجموعة من الاسئلة والمواضيع والمواضيع المقترحة لاخذ اراء عينة مكونة من ٧٠ فردا" ضمن فئات مستفيدة من هذه الخدمة ومختلفة في اتجاه التعامل من تاجر او بائع او مشتري او مستورد او مطلع على ابعاد هذه الخدمة الالكترونية وحتى ممارس لها او مستخدم للبطاقات الائتمانية .

وان الاسئلة الواردة في استمارة الاستبيان تم فيها اعتماد النظام الخماسي بتقييم اجابات افراد العينة ضمن خمس درجات وكانت (٥) علامات لاجابة اوافق بشدة و(٤) لاجابة اوافق و(٣) لاجابة محايد و(٢) لاجابة لا اوافق و(١) لاجابة لا اوافق بشدة.

وبعد اجراء التحليل الوصفي لاجابات عينة الدراسة على الاسئلة الاحدى عشر في الاستبانة لقياس درجة الوثوق والكفاءة الامنية للتجارة الالكترونية في العراق .

حيث تم استخراج المتوسط الحسابي لاجابات افراد العينة كما في الجدول ادناه :

ومن الجدول نجد ان اعلى متوسط حسابي كان (٤.٥٤٢٨٥٧) لاجابات العبارة رقم (٨) والتي تنص على (الرغبة في التوسع في نطاق التبادل التجاري عبر الانترنت بعد تعلم الطرق الامنة لمزاولتها) وبانحراف معياري مقداره (٠.٩٧٣٣٥١) وهذا يبين ان غالبية افراد العينة يفضلون التجارة الالكترونية في بيئة امنة ، كما توضح الاراء الى ان السبب الاساسي في التعامل هو الثقة والصحة وسلامة المعاملات التجارية من العبث او التزوير او التخريب .

ثم يتناقص المتوسط الحسابي حتى اقلها عند (٢.٤٧١٤٢٩) في اراء رقم (٧) والتي تنص على (التخوف من سرقة رقم البطاقة الائتمانية واعتماد مبالغ عليها دون علمي) وبانحراف معياري مقداره (١.٢٢٤٤٠٧) وهذا يدل على ان نسبة عالية من افراد العينة يرون ان امن المعلومات عبر الانترنت من اكبر العوائق لتوسيع واستمرار التجارة الالكترونية .

ثانيا" : الاستنتاجات :

لما كان النشاط التجاري يعتمد على توافر المعلومات اللازمة لانجاز معاملاته بسهولة ويسر فقد كان لزاما" ان تتأثر المعاملات التجارية بالتقدم المذهل في تقنية الاتصالات والمعلومات ايجابا" وسلبا".

كما آن وضع هذا السوق المتكامل على الانترنت هو راحة المستهلك في التسوق مع وجود اسعار منخفضة تنافس المتاجر التقليدية.

ان امن المعلومات عموما وامن التجارة الإلكترونية ؟ هو امن المعلومات المتبادلة على الخط ، ولذا ، وجدت جهات الحلول التقنية في سلسة التشفير مخرجا ملائما ، وتطور فن التشفير وحلوله الى المدى الذي امكن للمتخاطبين ضمان آن لا تفك رموز رسائلهم وتعاقداتهم ، لكن التشفير استلزم قواعد تشريعية في ميدان المعايير المقبولة حتى لا تتجاوز فائدته الايجابيات الى سلبيات حقيقية في ميدان انسياب المعلومات ونشرها .

التشفير ليس أرسلها حماية ضد العديد من طرق الهجوم المعروفة والشائعة والمتضمنة تلك الهجمات التي تستثمر التجهيزات الافتراضية او الانتهاكات في بروتوكولات الشبكات او البرمجيات بما فيها برمجيات التشفير ، وهكذا بزيادة التطور والتقدم في الاعمال الإلكتروني بما فيها التجارة الإلكتروني تبقى الحاجة الى طرق تقنية تشفير متطورة تكون خارج متناول الدخلاء.

عملية التشفير التي تحدثنا عنها تحقق الكثير في مجال أمن المعلومات لكن مع وجود الأخطار المحدقة لاتزال التجارة الإلكترونية تحتاج للكثير من التنظيم لتقليل عمليات النصب، ولاتزال الأنظمة والشبكات الموجودة بحاجة لاستخدام متطور لعلميات التشفير لضمان حماية خصوصية وأمن المستخدم.

ISSN-1994-697X

ثالثا" : التوصيات :

ومن اجل الوصول الى طرق سريعة لتداولها وتحليلها لاتخاذ قرار سليم مبني على الدقة والتحليل واعتمادا" على الدراسة الميدانية والاستنتاجات نجد انه يجب ان نساهم بقدر ما للتحول الى الاقتصاد الرقمي والذي يعتمد على الحاسبات وشبكة المعلومات والتجارة الالكترونية فقد تلمس بوادر ضعيفة لمزاولة التجارة الالكترونية في العراق ولزيادة فعالية تلك الخدمة عبر الانترنت وبعد ضمان الامنية الكاملة في التعامل يكون في تذليل العقبات التي تواجهها مثل تحسين شبكات الاتصال التي لا تزال ضعيفة ورديئة وتصميم قواعد المحاسبة المالية واعتمادها رسميا" ويكون ادخال هذه التقنية ونقلها لهذا البلد بالتجربة والتطبيق العملي .

كما ان تأخر او سوء استغلال خدمة الاتصال عبر الانترنت قد تؤدي الى ضياع عدد من الصفقات التجارية المهمة والتي تخدم شعبنا في البناء والتقدم.

وأن أهم أسباب استخدام الشركات للإنترنت هى ما يتعلق منها بالاتصال المباشر، فضلاً عن عاملي السرعة والسهولة، فالإنترنت بيئة التسويق الإلكتروني وفيما يلي بعض التوصيات المهمة :

١- القناعة والارادة السياسية
٢- التوسع في بناء وتكوين التكنولوجيا الرقمية .
٣- معرفة استراتيجيات التجارة الإلكترونية ومعرفة نطاقها وعلاقتها بعمليات اتمتة الأعمال وادارتها ، والتمييز بين طوائف وصور التجارة الإلكترونية ومعرفة كيف يمكن آن تطبق ومتطلباتها وتحدياتها.
٤- التركيز على التجارب المحلية والعربية والدولية والممارسات التطبيقية إلى جانب النواحي النظرية للاستفادة منها.

رابعا" : فكرة مستقبلية:

وتتمثل في توفر الموارد البشرية والمالية ووجود بنية متكاملة لتقنية المعلومات اضافة الى نشر الثقافة المعلوماتية ومجالات استخدامها من خلال الأجهزة الحكومية والخاصة على سبيل المثال ، وزارات الثقافة والإعلام، التربية والتعليم ، والجامعات والجمعيات العلمية ومجالس الغرف التجارية والشركات، والاستثمار في الأجيال المقبلة. وتشريع قوانين ضد مرتكبي الجريمة المعلوماتية لضمان وحماية برامج الحاسب الالي بصورة عامة وحماية التبادل التجاري بصورة خاصة.

وزيادة المعرفة العلمية والتقنية والخبرة في مجال الحاسب والانترنت لحماية التبادل التجاري من الغش والاحتيال الالكتروني.

الخلاصه:

يتطرق البحث الى فكرة حديثة بحاجة الى مزيد من البحث العلمي لاغناء المكتبة العربية ، حيث ان البحث قذ مزج بين ثلاث ميادين في ميدان التجارة الالكترونية وهي الميدان الاقتصادي وتقنيات التشفير وشبكة الانترنت.

فقد فرضت التطورات التكنولوجيه الهائله واقعا جديدا لابد من التعامل معه وخاصه في مجال الاتصالات الحديثه وهي التجارة الالكترونية حيث تعتبر احد اهم واكثر الخدمات شيوعا" لانها وفرت القدرة على البيع والشراء في أي زمان او مكان ، لكن ما تزال التجارة الالكترونية في قطرنا حلم مستقبلي بطئ التحقق والانتشار رغم الرغبة الملحة لكل فرد او هيئة تجارية في التوسع لهذه الخدمة وذلك بسبب المخاوف في حفظ البيانات المصرفية وسرقة بطاقات الائتمان .

وقد تناول البحث للجانب الاكثر اهمية في هذه الخدمة وهو التشفير والتواقيع الرقمية والبصمة الالكترونية لتحقيق اتصال امن مع مواقع التسوق عبر الانترنت وضمان موثوقية التعامل التجاري ، والرغبة الحقيقية في مزاولة هذه الخدمة لما توفره من سهولة وسرعة في التعامل .

وقد اعتمدت اراء عينة من الافراد ضمن اسئلة استمارة استبيان واجراء التحليل الوصفي للاجابة.

ISSN-1994-697X

المصادر

١- أ.د.عوض حاج علي احمد و د. عبد الامير خلف حسين ، " امنية المعلومات وتقنيات التشفير" / رئيس جمعية النيلين / جامعة الزرقاء الاهلية ، دار الحامد للنشر والتوزيع ، الاردن –عمان ، ٢٠٠٥م.

٢- المحامي عمر حسن المومني ، "التوقيع الالكتروني وقانون التجارة الإلكتروني" / ماجستير قانون تجاري / بريطانيا ،دار وائل للنشر ،٢٠٠٣م ، عمان.

٣- مجلة البنوك الاردنية / التجارة الإلكتروني ، الاعداد ٧و٨ و٩ - ١٩٩٩

٤- المنصف قرطاس ، "التجارة الإلكترونية والاشكالات التطبيقية المطروحة"، ، مقال منشور ضمن كتاب التجارة الإلكترونية والخدمات المصرفية والمالية عبر الإنترنت ، منشورات اتحاد المصارف العربية ،بيروت ، ٢٠٠٠،ص٢١٨.

WWW.SAFOLA.COM -٥-Copyright © 2000 Smart Articles For OnLine Activity Arabic Web Magazine for Internet Security , Privacy Protection & Computers

٦- شبكة عربيات / مجلة عربية الكترونية ، "مفاهيم التشفير والتوقيع الرقمي" ، ،٢٠٠١.

٧- علي عبد الامير ، "من عالم التعمية الى التشفير الرقمي" ،٢٠٠٣.

٨- " أ.د.عوض حاج علي احمد / رئيس جمعية النيلين ود. عبد الامير خلف حسين / جامعة الزرقاء الاهلية ، " خوارزميات التشفير"، دار الحامد للنشر والتوزيع ، الاردن –عمان ، ٢٠٠٥م.

٩- د. محمد طاهر نصير و د. محمد طاهر نصير ، "التسوق الالكتروني "، ، عمان ، دار الحامد للنشر ،٢٠٠٥م.

١٠- اسامة احمد المناعة /ماجستير قانون و جلال محمد الزعبي /ماجستير قانون ، وصايل فاضل الهواوشة/ماجستير قانون ، "جرائم الحاسب الالي والانترنت.. دراسة تحليلية مقارنة"، ، عمان –الاردن دار وائل للنشر ،٢٠٠١.

١١- د. محمد حماد مرهج الهيتي "جرائم الحاسوب .. ماهيتها ، موضوعها ، اهم صورها والصعوبات التي تواجهها" ، ،٢٠٠٥

١٢- وليد الزيدي ، "التجارة الالكترونية عبر الانترنت" / عمان – دار المناهج للنشر والتوزيع .

١٣- مدونة أحمد الهاشمي: أرشيف الأمن والحماية ، "التشفير بالمفتاح غير المتناظر" ، الاثنين ٢٧ يونيو ٢٠٠٥

١٤-عادل عبد الصادق ، "قانون التوقيع الالكتروني : نحو مجتمع معلوماتي في مصر" ، ملفات الأهرام ، الاثنين ٢٦ يوليو ٢٠٠٤ العدد ١٢٧

ISSN-1994-697X