استخدام توابع رياضية معقدة وتطبيق خوارزميات التشفير في السلاسل المحرفية اعتماداً على النمذجة الرياضية.

د. محمد جمال حمندوش*

د. محمد دبش**

ديما دبابو***

(تاريخ الإيداع 29 / 6 / 2020. قُبِل للنشر في 26 / 8 /2020)

□ ملخّص □

تتم عملية الموازنة اعتماداً على النمذجة الرياضية وسلسلة محارف نصية متمثلة بعدة توابع رياضية متغيرة لحل مشكلة الموازنة بين عاملي الكلفة الحسابية والمتمثلة بزمن تنفيذ خوارزمية التشفير (Encryption Algorithm) ومعامل الأمان (Safety Coefficient) المرتبط بطول مفتاح التشفير وذلك بحساب عدد العمليات المنفذة في الثانية الواحدة والتي تعرف ما يسمى بتعقيد الخوارزمية وطول المفتاح اللازم لعمليتي التشفير(Encryption) وفك التشفير(Encryption) بالإضافة إلى التركيز على عدة عوامل أساسية أثناء عملية التنفيذ وهي المساحة التخزينية (Storage Space) وسرعة المعالجة(Processing Speed) زيادة السرية (Confidentiality) .

يتم التركيز على النقطة الحدية التي يجب اعتبارها نقطة توافق بين عامل السرية (الوثوقية) (Confidentiality) وعامل السرعة (Speed Factor) وتحدد هذه النقطة بحسب طبيعة وحجم البيانات المرسلة وذلك من خلال استخدام خوارزميات التشفير وتوابع رياضية متغيرة وذلك لتحويل البيانات والمعلومات إلى خليط من الرموز والأرقام والأحرف باستخدام قواعد التشفير(Cryptography).

* استاذ مساعد. قسم الرياضيات. كلية العلوم. جامعة حلب. حلب. سورية

**استاذ مساعد. قسم الرياضيات. كلية العلوم. جامعة حلب. حلب . سورية

***طالبة دكتوراه. قسم الرياضيات. كلية العلوم. جامعة حلب. حلب. سورية

Use complex mathematical minions and apply encryption algorithms in literal strings based on mathematical modeling.

Dr. Mohamed Jamal Hamandoush*
Dr. Mohamad Dababsh**
Dima Dababo***

(Received 29 / 6 / 2020. Accepted 26 / 8 /2020)

□ ABSTRACT □

The balancing process is based on mathematical modeling an a series of text phs represented by several variable mathematical sequences to solve the problem of balancing the calculation cost factors of the time of implementation of the encryption algorithm

this process, a string of text characters represented by several variable mathematical consequences is divided into solving the problem of the balance between the mathematical cost factors represented by the time of implementation of the encryption algorithm and the safety coefficient associated with the length of the encryption key by calculating the number of operations executed per second that know what The complexity of the algorithm and the key length required for the encryption and decryption processes, in addition to focusing on several key factors during the implementation process, are called Storage Space and Processing Speed, Increasing Confidentiality.

Emphasis is placed on the marginal point that must be considered a compatibility point between the confidentiality factor and the speed factor, and

this point is determined according to the nature and size of the data transmitted through the use of cryptographic algorithms and variable mathematical functions to convert data and information into a mixture of symbols And numbers and letters using Cryptography rules.

* **Associate Professor, Dept. of Mathematics, Faculty of Science, University of Aleppo, Syria**
** **Associate Professor, Dept. of Mathematics, Faculty of Science, University of Aleppo, Syria**
*** **Postgraduate Student (MSc.), Dept. of Mathematics, Faculty of Science, University of Aleppo, Syria**

مقدَّمة.

تم استخدام علم التشفير مُنذ أكثر من أربعة ألاف سنة وله دور فاعل في سنوات القرن العشرين ترافق مع تغييرات جذرية في طرق التخزين ونقل المعلومات وتقنيات الحصول عليها، ولكن متطلبات أمن المعلومات من حيث الخصوصية وسرية المعلومات(Confidentiality)، وتوفر المعلومات للأطراف المخولة(Availability)، وكمال وسلامة المعلومات(Integrity) التي لم يطرأ عليها أي تغيير من حيث تخزين المعلومات أو نقلها عبر شبكات الاتصال من خلال الحفاظ على سرية المعلومات دون تغيير وصلاحيات قبول الأشخاص المخول لهم بالحصول على المعلومات.

تشمل عمليَّة التشفير(Encryption) أنواع عديدة من خوارزميات أمن البيانات والمعلومات. يُعد علم التشفير علم ضخم بما يحتويه من معلومات وأفكار وطرق وسّبل في جعل المعلومات أياً كانت: رسائل إلكترونية ، ملفات ، عبارات أو رموز مّشفرة هذا يتطلب تقنية عاليَّة في معرفة تجزئة السلاسل وإتباع منهجية مُعينة لتجزئة سلسلة المحارف النصية بطريقة تسعى إلى العشوائية في كل عمليَّة يتم فيها تنفيذ الخوارزمية المُقترحة بعدها في الخطوة التالية يتم تشفير كل سلسلة جزئية مشفرة باستخدام طرائق التشفير المّختلفة,إضافة إلى أن خوارزميات التشفير تحتاج كل منها إلى مفتاح خاص بها، وهذا يزيد من صعوبة وتعقيد سلسلة المحارف النصية المشفرة من أجل الحفاظ على أمن البيانات والمعلومات، بعدها تتم عمليَّة دمج السلاسل مّغلفة بغلاف لا يستطيع أحد فهمه. أيضاً يُعرف علم التشفير بصيغة أخرى على أنه وسيلة لاستبدال رسالة أو مستند حيث لا يمكن معرفة محتوياتها وذلك بالترميز الخاص بها. ويقصد بالترميز هو عمليَة تحويل النص الصريح (Plain Text) إلى رموز.

أهميَّة البحث وأهدافه.

تأتي أهمية هذا البحث من خلال إمكانية تطبيق طريقة منهجية معينة للتشفير وتطبيقها على نصوص حقيقة، أما أهداف البحث فنختصر في:

1- دراسة أهم الخوارزميات المستخدمة في التشفير وفق الأسس الرياضية المبنية عليها مع التركيز على الخوارزميات المتقدمة بحسب كفاءتها في العديد من التطبيقات مثل خوارزمية (RSA).

2- دراسة مسألة الأمثلة في طرق التشفير متعددة الأهداف والطرائق الرياضية المستخدمة في حلها بما فيها طرائق البحث الحدسية.

3- إيجاد النموذج الرياضي الموافق للمشكلة المطلوب حلها للموائمة أو الموازنة بين عاملي الكلفة والزمن، ومن ثم بناء خوارزمية أمثليه قابلة للتطبيق بأقل عتاد حاسوبي ممكن.

4- تطبيق النموذج الرياضي والخوارزمية المقترحة. وذلك من خلال تصميم برنامج واختباره على مجموعة من الملفات النصية ذات أطوال مختلفة.

مفهوم علم التشفير (Concept of Encryption).

علم التشفير هو عباره عن خوارزميات لأمن المعلومات والبيانات. تتم عمليَّة التواصل وتبادل المعلومات بين الطرفين أو أكثر، وذلك باستخدام قواعد التشفير(Cryptography)الخاصة مع مفتاح سري وذلك باستخدام رمز أو مجموعة

من الرموز في الرسالة الأصلية مع تسلسل رمز أو أكثر من رموز النص المشفر، ونجاح العديد من العمليات يعتمد بشكل كامل على سرية تبادل الاتصال بين المرسل (Cryptographer) والمستقبل (Interceptor).[1]

يتضمن علم التشفير أربعة أجزاء رئيسية:

1.التشفير وفك التشفير(Encryption & Decryption)

وهي تستخدم لتحقيق سرية البيانات والمعلومات وجعلها بصورة مخفية عن طريق عملية التشفير. أمَّا فتح الشفرة (عمليَّة فك التشفير) هي عكس عملّية التشفير وهي إعادة البيانات والمعلومات إلى صيغتها الأصلية.[1]

2التوقيع الرقمي(Digital Signature) .

وهو جزء مميَّز(Unique) للشخص ويخدم وسيلة للتعرف ويستخدم للتخويل،(Authorization) والتثبيت (Validation) باستخدام المعلومات الإلكترونية فإن فكرة التوقيع تحتاج إلى إعادة تحديد وهي أن تكون ببساطة شيء ما مميَّز للموقع(Singer) وتكون مستقلة عن المعلومات المَّوقع عليها.[1]

3.البصمة(Hashing).

وهي تستخدم لتحقيق سلامة البيانات(Data Integrity) وحفظ المعلومات من التغيير(حذف_أضافة_تعديل) من قبل الأشخاص غير المصرح لهم بذلك، وتعتبر أحد الأدوات المستخدمة في الحفاظ على أمن المعلومات للوصول إلى أعلى مستوى من الاحترافية والجودة.[1]

4.عدم التنصل(Non-repudiation).

يقصد بعدم التنصل منع المرسل أو المستقبل من إنكاره الرسالة المنقولة وبالتالي عندما يتم إرسال الرسالة يستطيع المستقبل الإثبات بأن الرسالة تم إرسالها فعلاً من قبل المرسل المزعوم. بشكل مشابه عند استقبال الرسالة يمكن للمرسل أن يثبت أنه تم استقبال الرسالة فعلاً من قبل المستقبل.

أنواع مفاتيح التشفير (Types of encryption keys) :

تُعتبر مفاتيح التشفير المحور الأساسي لعلم التشفير حيث تتميز كل طريقة تشفير بمفتاح خاص بها للحفاظ على أمن البيانات والمعلومات وهذا المفتاح يكون معروف من قبل المُرسل (Cryptography)والمستقبل (Interceptor). ومن أنواع مفاتيح التشفير:

1.المفتاح العام (Public-Key): يستخدم هذا المفتاح في تشفير الرسائل, ويكون عادة من أساسيات عمليَّة التشفير، وهذا المفتاح يكون معروف من قبل أي شخص ولكن لا يستطيع أحد فك الرموز لتلك المعلومات، لأنه يحتاج إلى الرقم السري لإتمام عملية فك تلك الرموز والحصول على المعلومات المطلوبة[2] .

2.المفتاح الخاص (Private-Key) : يُعتبر هذا المفتاح بالمفتاح المُكّمل للمفتاح العام، وهو يعتبر بمثابة هوية إلكترونية تُمكن مستخدمها من فك أي معلومة مشفرة مرسلة إليه على أساس المفتاح العام، ولذلك يجب علينا الاحتفاظ بالمفتاح الخاص سراً [2] .

خوارزميات التشفير:

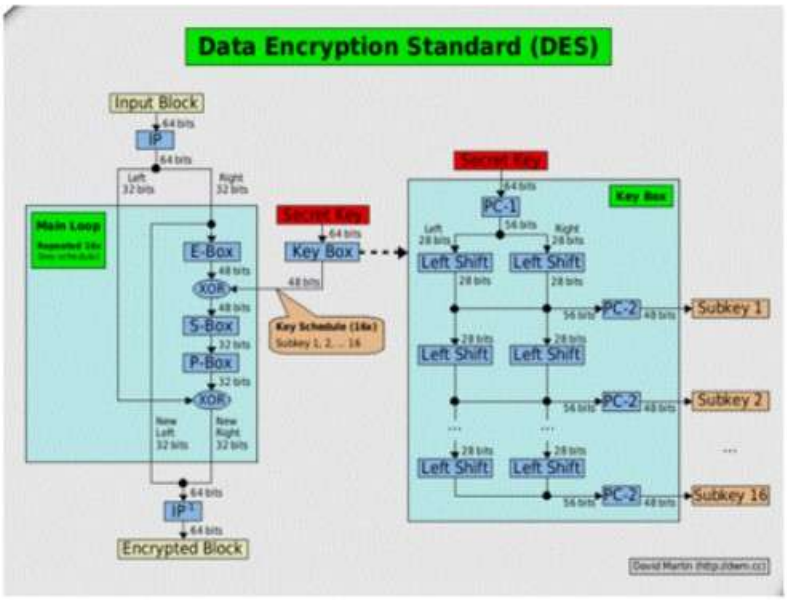
تم تطبيق خوارزميات التشفير المعقدة والمختلفة على سلسلة المحارف النصية على أساس وضع قياسات (Standards)مختلفة لكل سلسلة جزئية بُغية استخدام خوارزميات التشفير المتُعددة (Multiple Encryption Algorithms) في التطبيق العملي بشكل فعال.

من أهم خوارزميات التشفير المُستخدمة:

1 طريقة تشفير معايير البيانات القياسية (DES):

تعتمد هذه الخوارزمية على نظرية المفتاح المُتناظر (Symmetric Key) أي استخدام نفس المفتاح عند التشفير وفك التشفير، حيث أن حجم النص المُدخل ثابت (64bit)، أمَّا حجم مفتاح التشفير المُستخدم (56bit)، وتعمل هذه الخوارزمية على ثلاث مراحل:

1. معالجة مفتاح التشفير: حيث يتم هنا استخدام جداول وعمليات متسلسلة يتم فيها استخدام التدوير (Rotation) والتبديل (Permutation) لينتج عنها أخيراً(16) مفتاح ليُستخدم في المراحل اللاحقة[3].
2. تطبيق الخوارزمية: في هذه المرحلة يتم استخدام جداول وعمليات متسلسلة يتم فيها استخدام التدوير (Rotation) والتبديل (Permutation) كما في المرحلة السابقة، لكنها هنا تتم على النص المراد تشفيره وليس على مفتاح التشفير كما في المرحلة السابقة. في هذه المرحلة تستخدم جداول الاستبدال (Substitution)[3].
3. في هذه المرحلة تتم عمليَّة عكسية لجزء ممَّا تم في المرحلة الأولى، حيث يتم تبديل النص باستخدام جداول التبديل (Permutation) ونلاحظ عمليَّة فك التشفير تتم بطريقة معاكسة لعملية التشفير مع فروق بسيطة جداً[3] .



الشكل (1)

2. طريقة التشفير ذاتية التوليد(Auto-Key Cipher).

تقوم هذه الطريقة على تكوين مفتاح واحد مُتفق عليه بين المرسل والمستقبل مسبقاً. للقيام بعملية التشفير يقوم المرسل بكتابة النص الصريح ووضعه في جدول في الصف الأول ويكتب تحت كل حرف من حروف النص الأصلي مواقع هذه الحروف حسب الترتيب الأبجدي في الصف الثاني وفي الصف الثالث وفي أول عمود يُكتب المفتاح المتفق عليه، وفي العمود الثاني من نفس الصف يُكتب موقع الحرف الأول (المكتوب في الصف الثاني في العمود الأول)، وفي العمود الثالث يُكتب موقع الحرف الثاني وهكذا حتى نهاية الصف. ثم يقوم بجمع كل رقمين متقابلين من الصف الثاني والثالث ويوجد باقي قسمة الناتج على عدد الأحرف الأبجدية فيكون الرقم الناتج هو موقع الحرف المُشفر حسب الترتيب الأبجدي. أمَّا المُستقبل فيقوم بعملية عكسية لعملية التشفير للحصول على النص الأصلي.[5]

3.طريقة التشفير بالضرب(Multiplicative Cipher) .

هذه الطريقة تقوم بعملية التشفير عن طريق ضرب كل حرف من حروف النص الأصلي بالمفتاح المُتفق عليه وإيجاد باقي قسمة ناتج الضرب على/28/. أمَّا في الخطوة التالية والتي تُمثل عملية فك التشفير تتم بضرب كل حرف من أحرف النص المشفر بالنظير الضربي للمفتاح وإيجاد باقي قسمة الناتج على/28/.[7]

4.طريقة التشفير الإزاحة(Substitution Cipher) .

تعتمد هذه الطريقة على خطوات متكررة في التعويض عن أحرف النص الأصلي بأحرف بديلة وفق قاعدة معينة للحصول على النص المشفر والتبديل ما بين موقعها لإعطائها ترتيباً مختلفاً في هذه الحالة نسعى للحفاظ على سرية البيانات المعلومات التي تم تشفيرها ومن ناحية أخرى هو عملية استبدال للقيم والعناصر المحددة في رسالة ما أو أي بيانات أخرى وتتم هذه العملية على مستوى الحروف من الناحية العملية.[6]

5.طريقة التشفير (RSA).

تعد هذه الطريقة من أوائل وأكثر نظم التشفير المعتمدة على المفاتيح غير متناظرة استخداماً. لقد تم تطوير هذا النظام من قبلAdShamir Ron Rivest، &Leonard Adleman. هذه الخوارزمية مستخدمة في بروتوكولات التجارة الإلكترونية على نطاق واسع، وهي أمنة طالما أن المفتاح طويل جداً. على سبيل المثال (1024bit). وتعتمد بشكل كبير على أنه لا يوجد خوارزمية لتحليل عدد لعوامل بسرعة كافية.[4]

الدّراسات التجريبيّة (Experimental Study).

تناولت هذه الدَّراسة التجريبية تـجزئة سلسلة محارف نصية مُؤلفة من أكثر من (350) محرف إلى خمس سلاسل جزئية باستخدام طرائق تشفير مختلفة وتشفيرها وهي طريقة التشفير الأولى (DES) للسلسلة الجزئية الأولى والثانية طريقة التشفير(Auto-Key) للسلسلة الجزئية الثانية أما طريقة التشفير الثالثة فيتم تشفيرها بطريقة الضرب (Multiplication Cipher) ومفتاح هذه الخوارزمية له طريقة تشفير خاصة به. ويتم تشفير السلسلة الجزئية الرابعة بطريقة الإزاحة(Substitution Cipher) وأخيراً يتم تشفير السلسلة الجزئية الخامسة بطريقة تشفير(RSA) وبعدها يتم تسمية كل سلسلة جزئية مشفرة باسم جديد ثم نقوم بعمليَّة دمج السلاسل الجزئية المشفرة بطرائق التشفير المقترحة في هذه الدراسة التجريبية لتشكيل سلسلة المحارف النصية المشفرة، والمثال التالي يوضح آلية عمل طريقة تجزئة سلسلة المحارف النصية وتشفيرها.

مثال (1). ليكن لدينا النص التالي:

Do you want to have the power to release your negative emotions, pains, anxieties, and traumas? Are you tired of not moving forward in your career, health, and relationships?
I help to empower you to reach greater levels of wellness and success through my speaking, teaching, and counseling sessions.
These sessions are supported by my educational television Telly award-winning DVD's, life-changing book, "Quest for the Empowered Self," and music and audio CD's I've created to ensure your long-term success
Because my products and services (live presentations and counseling sessions) have such a high percentage rate of success, every product and service purchased comes with a money back guarantee.
I have offered this guarantee for eight years, and still, nobody has asked for their money back to date. Read below and visit the EFT store above to see which products and services will serve you best.

I often utilize the highly effective technique EFT (Emotional Freedom Technique) that uses the tapping on acupuncture points on the body to release negative emotions, trauma, and pain stored in the body and mind.

Chinese acupuncture has been practiced for at least 3,000 years. EFT combines this ancient wisdom with cognitive psychology and is an impressive technique for eliminating emotional and physical problems by rebalancing the energy system of the body.

It is a simple, rapid, respectful way of healing a wide variety of fears, memories, and disturbances. I am EFT Certified.

يتم تشفير النص الصريح المُؤلف من أكثر من (350) محرف وذلك بتجزئتها إلى خمس سلاسل جزئية وتشفير كل سلسلة جزئية بطريقة تشفير وعند الانتهاء من عملية التشفير يتم دمج السلاسل الجزئية للحصول على نص مشفر،وعندها خوارزمية تجزئة سلسلة المحارف النصية المُشفرة تعطى بالشكل التالي:

cipher_text1 =v|þ* §Á

cipher_text2=~ØÏâ” ” ã • ^ É×Û…” ÜÍ…• ßæÜ×’ ” ã • ’ ×ÑÑÆÔØ…™ëäç’ Ž ÓÌÈÕÝßÛ …..ÒÜãÝØÝáŸL • ÑÊ×áŸL • ÏæáÎÙÝÎØŸL • ÏÒ„ ” æÓÖâÎÔ²I*a³×…™ëä• ” ÝÛ×É„ • Õ† Ž Ýã” • Üåß×Õ‡ † ÕáéØÓÖ„ ‰Ž ™ëäç’ ƒ ÄÓ×Ê×ž L^ ÍÆÍàÜ” L • ÏÒ„ ’ ×ÑÍÕÝØ ÝáÛÑÙã²I*iiˆÍÑÜ□”ã□…ÒÝßæÜ×’™èä•”ã□’×ÆÄËˆ‡Ù×ÆÕÙ×’ŒÑÛÛÑß“□Õ†— ÜÑØÚÓØæ“□ÏÒ„“èØÆÈØæ“”ÜÚáäÜÏˆ□æ™“ãÕÆÌÔ×Õ“L”ÙÆÄËÑ×Õ“6* • ÏÒ„ƒÒäã áØÑÕ×Õ‡“ØØæÜØÝá¡Nt¼ÍØØ…“ØØæÜØÝá“□Ó×…“èåàßáæÙÉ„„Û™□æ™…ÉÙØÄ ÕÝØÝÏÍŒ”ÙÑÑÛßÜÜØÝŽ t'ÑØå™□ØØÓÖ‘¤à×Ü××Õ‡

cipher_text3 =ÜZÜþ%4FàôßÊÃ;µØ§ÑßÑà® í4à73Ã%,àÊ -à,ØÃàãûAÃ-Ã¼àEÃôÊ4à§¼àû3%ßµà§¼à§3¼ßàÕÜþ%àÿþ:Ãàµ-Ã§,Ã¼ààÃ%3-ÃàO3-à ôÑ;,Ã-ûà%3µµÃ%%BFàÎÃµ§3%ÃàûOà-¼3µ,%à§¼à%Ã-:ßµÃ%àôß:Ãà-Ã%Ã,§,ß %à§¼àµ3%ÃôßÑà%Ã%%- àØ§:Ãà%3µØà§àØßÑØàÃ-µÃ,§ÑÃà-§,ÃàÊà%3µµÃ%%4àFàÃ:Ã-Oà¼3µ,à§¼à%Ã-:ßµ Ãà3-µØ§%Ã¼àµûÃ%àAß,Øà§àûÃOà®§µíàÑ3§-§,ÃÃBàÿàØ§:ÃàÊÊÃ-Ã¼à,Øß%àÑ3§- §,ÃÃàÊ-àÃßÑØ,àOÃ§-%4

cipher_text4 =-n{q-€ • vyy9--{|o|q†-un€ -n€ xrq-s|□- • urv□-z|{r†-onpx- • |-qn • r;-_rnq-ory|„-n{q-ƒv€ v • - • ur-RSa-€ • |□r-no|ƒr- • |-€ rr-„uvpu-}□|q,p • € -n{q-€ r□ƒvpr€ -„vyy-€ r□ƒr-†|,-or€ • ;-V-|s • r{-, • vyv‡r- • ur-uvtuy†-rssrp • vƒr- • rpu{v~,r-RSa-5Rz| • v|{ny-S□rrq|z-arpu{v~,r6- • un • -,€ r€ - • ur- • n}}v{t-|{-np,},{p • ,□r-}|v{ • € -|{- • ur-o|q†- • |-□ryrn€ r-{rtn • vƒr-rz| • v|{€ 9- • □n,zn9-n{q-}nv{-€ • |□rq-v{- • ur-o|q†-n{q-zv{q;--P

cipher_text5=)yT • T+},^‹^y, • ^ŸT+} • +TTy+‹Ÿ}, •),To+wdŸ+} • +ž T} • • +X+nT}Ÿ • (++6V]2+,dA)yT • + •) • +}y,)Ty • +^) • odA+^) • +,d‰y) •)eT+‹ • n,dž d‰n+}yo+) • +}y +)A‹ŸT • •)eT+ • T,y)a^T+wdŸ+Tž +)A)y} •)y‰+TAd •)dy}ž 6+}yo+‹n •),}ž +‹Ÿdž

TA • +n+ŸT}ž }y,)y‰+ • T+TyTŸ‰n+ • n • • TA+dw+ • T+don(+ • +) • +}+ •)A‹ž TX+ Ÿ}‹)oX+ŸT • ‹T, • w^ž +ˆ}n+dw+T}ž)y‰+}+ˆ)oT+e}Ÿ)T • n+dw+wT}Ÿ • X+ATAdŸ) T • X6+}yo+o) • • ^Ÿ}y,T • (+++}A+V]2+CTŸ •)w)T

الشكل (4): تجزئة وتشفير سلسلة المحارف النصية للدراسة التجريبية

أمَّا نص فك التشفير، في هذه الخطوة يتم فك تشفير كل سلسلة جزئية مشفرة ودمجها للحصول على النص الأصلي الذي يُمثل سلسلة المحارف النصية يصبح بالشكل التالي:

dec_text1 = Do you
dec_text2 =want to have the power to release your negative emotions, pains, anxieties, and traumas? Are you tired of not moving forward in your career, health, and relationships?
I help to empower you to reach greater levels of wellness and success through my speaking, teaching, and counseling sessions. These sessions are supported by my educational television Telly award-winning
k = 183
dec_text3 =DVD’ s, life-changing book, “ Quest for the Empowered Self,” and music and audio CD’ s I’ ve created to ensure your long-term success.
Because my products and services (live presentations and counseling sessions) have such a high percentage rate of success, every product and service purchased comes with a money back guarantee. I have offered this guarantee for eight years,
dec_text4 = and still, nobody has asked for their money back to date. Read below and visit the EFT store above to see which products and services will serve you best. I often utilize the highly effective technique EFT (Emotional Freedom Technique) that uses the tapping on acupuncture points on the body to release negative emotions,trauma, and pain stored in the body and mind
dec_text5 =hinese acupuncture has been practiced for at least 3,000 years. EFT combines this ancient wisdom with cognitive psychology and is an impressive technique for el iminating emotional and physical problems by rebalancing the energy system of the body.
It is a simple, rapid, respectful way of healing a wide variety of fears, memories,
and disturbances. I am EFT Certified.
Ans=0

الاستنتاجات والتوصيات:

استنتاجات(Conclusions)

إن دراسة مسائل التشفير تتطلب الإلمام بالجانب الرياضي إلى حد كبير وتعتبر نظرية الأعداد هي المصرف الأول الذي يصب في نظرية التشفير، كما أن ازدياد الحاجة لرفع سوية خوارزميات التشفير كان وراء تطور نظرية الأعداد، وبناءً عليه سيكون لهذه الدراسة أثراً من الناحية النظرية بشكل أو بآخر على العلوم الرياضية. من جهة ثانية، يمكن أن توفر هذه الدراسة تطبيقات قابلة للتفعيل على الأنظمة الحاسوبية أو الأجهزة المحمولة بأقل عتاد حاسوبي ممكن، وبالتالي زيادة أمان نقل المعلومة بين المرسل والمستقبل وشبكات الاتصال بشكل عام أو شبكات الاتصال المحلية.

الأعمال المستقبلية(Future business) .

سنقوم بدعم جميع منتجات التشفير اللازمة لكافة أنواع الرسائل النصية والمحرفية للحفاظ على أمن البيانات والمعلومات التي تتجاوز عشرات الألاف الكيلومترات كما هو الحال في شبكة الإنترنيت. حيث يتم تطبيق على عدة أنظمة حاسوبية من شركات وبنوك وفي المجالات العسكرية والسياسية من خلال تخزين المعلومات وضمان الأمن والسرية في نقل المعلومات خصوصا بعد التطورات الهائلة التي طرأت على عناصر وتقنيات تخزين المعلومات المستخدمة فيها.

References.

[1] Diaa Salama, Hatem Abdual Kader, and Mohiy Hadhoud, 2011-Astudy design and data encryption algorithm Transmitted, Jazan University, Kingdom of Saudi Arabia.

[2] Jonathan Katz, 2010-Digital Signatures (Advances in Information Security), Department Of Computer Science, University of Maryland, A.V.E Williams Bldga.

[3] Czeslaw Koscielny, Miroslaw Kurkowski and Marian Srebrny (Dec 3, 2013) - Modern Cryptography Primer: Theoretical Foundations and Practical Applications, Springer Heidelberg Dordrecht London New York.

[4] Burnett, Steve; Paine, Stephen, 2010 -RSA Security's Official Guide to Cryptography, New York McGraw-Hill Professional.

[5] Mohamed A.Haleem, Member IEEE,2007-Opportunistic Encryption: A Trade-OFF between Security and throughput in Wireless Networks.

[6] Baiquan Lu, Yuan Cao, Min Jie Yuan, Jianzhen Zhou, 2007-Reference Variable methods of solving min-max optimization problems, spring Science + Business Media, China.

[7] Divya Kumar,Divya Kashyap,K.K.Mishra and A.K.Misra,2010-Security Vs Cost: An Issue of Multi-objective optimization for choosing PGP Algorithms,department of computer Science and Engineering Motilal Nehru National Institute of Technology Allahabad,India.