مجلة جامعة بابل / العلوم الصرفة والتطبيقية / العدد (١) / المجلد (٢٤) : ٢٠١٦

تشفير البيانات الحية المنقولة بين نقطتي اتصال

علي هادي حسن

كلية العلوم – جامعة بابل

Alihadihassan2010@yahoo.com

الخلاصة

يهدف هذا البحث إلى تصميم منظومة برامجيات لتراسل وحماية البيانات والمعلومات الحية المنقولة عبر قناة اتصال على طرفيها حاسبتين احدهما مرسلة والأخرى مستقبلة ، وذلك ببناء برامجيات منخفضة المستوى تتعامل مع منافذ الحاسبة الداخلية والخارجية لتناقل البيانات ، كذلك تصميم وبناء منظومة برامجيات توجد آلية لحماية هذه البيانات والمعلومات المهمة والسرية من أعين المتطفلين والجواسيس باستخدام بعض أنظمة التشفير وفك الشفرة.

تم تنفيذ طريقة لبرمجة المنافذ وبالأخص المنفذ المتوازي وتراسل البيانات خلال هذا المنفذ ثم نقلها من والى المعالج والذاكرة الرئيسية وبالعكس لغرض معالجتها. بعد ذلك صممت ونفذت طريقة لمعالجة وحماية هذه البيانات وذلك ببناء منظومة لتشفير هذه البيانات باستخدام عدة طرق مختلفة التعقيد هي نظام التشفير الجمعي ونظام التشفير الضربي وهي أنظمة تشفير تعويضية ونظام تشفير متعددات الحدود وهو نظام تشفير انسيابي ونظام تشفير النابساك بطريقة ماركل–هيلمان في الحاسبة المرسلة . ثم تمت عملية فك الشفرة لهذه الطرق بعد إعطاء مفتاح فك الشفرة واسترجاع البيانات والمعلومات الواضحة مباشرة في الحاسبة المستقبلة.

إن المنظومة البرمجية التي تم تصميمها وبنائها هي منظومة كفوءة وفعالة وسهلة الاستخدام ولها القابلية على تراسل وخزن البيانات المرسلة والمستقبلة وتوثيقها بسرعة عالية.

الكلمات المفتاحية: تراسل بيانات حيه خلال المنفذ المتوازي، منظومة برمجية لتشفر وفك الشفرة.

Abstract

This research aims at designing a software system for communication and protecting a data and live information transmitted through a communication channel on both ends one is sender and the other is receptor by building a low-level software to deal with internal and external ports for data transfer. In addition to design there is a software mechanism for the protection of this data and important information and confidentiality from spies using some encryption systems and decoding.

We implemented a method for programming the parallel port and then transported data to and from the processor and main memory, and vice versa for the purpose of processing. We designing, building and implement a methods to process and the protect this data by using an encryption system of a collective of several different complexity encryption methods like additive, multiplicative, stream cipher and Nabsak by Markle-Hillman in a sent node (computer). These methods are decoded after giving the public key and retrieving a clear information directly into the receiving node (computer).

The software system that has been designed and constructed is efficient, effective and easy to be used and it has the ability to transmit and store sent and received data and document them at high speed.

Key Words: Transported a Live Data through Parallel Port, Software System for Encryption and Decoding Methods.

1– المقدمة

إن من احدث التطورات في مجال الحاسبات استخدامها في منظومات تراسل البيانات والمعلومات وطرق خزنها ومعالجتها مثل الرسائل الالكترونية والبريد الالكتروني وأنظمة قواعد البيانات والمعلومات ومعالجة الصور الرقمية وأنظمة تمييز ومعالجة الصوت، حيث أصبحت الحاسبات جزءاً مهماً من مكونات شبكات الاتصالات التي تمر خلالها معظم بيانات ومعلومات الشبكات مما تطلب إيجاد آلية لنقل وحماية هذه البيانات ومعلومات.

١–١ : أمنية البيانات

إن وسائل وطرق أمنية البيانات والمعلومات عديدة ونشطت أخيراً أنظمة تشفير البيانات التي تحتوي على أنواع مختلفة الشفرات التقليدية والحديثة، حيث تظم أنظمة التشفير التقليدية الشفرات التعويضية والشفرات الابدالية أما نظم التشفير الحديثة فتظم أنظمة التشفير القياسي للبيانات والتشفير الانسيابي والمفتاح المعلن [Beker and Piper; 1982].

تهدف عملية التشفير Encipher Operation إلى تمويه المعلومات المهمة بطريقة ما، بحيث يصبح معنى هذه المعلومات غير واضح للشخص غير المخول (المعترض)، تدعى المعلومات التي تريد إخفائها قبل عملية التشفير بالنص الواضح Plaintext، وتدعى عملية التمويه بعملية التشفير Encipher ، ويدعى النص الناتج بعد عملة التشفير بالنص المشفر Ciphertext أو Cryptogram.

تعرف مجموعة الخطوات التي يستخدمها معالج التشفير لتشفير النص الواضح بخوارزمية التشفير Encryption Algorithm ، ويعتمد عمل هذه الخوارزمية على مفتاح التشفير Key الذي يدخل مع النص الواضح إلى الخوارزمية. هذا المفتاح يكون معرفاً للمستلم وبه يستطيع استعادة النص الواضح من النص المشفر [Tarish; 2000].

إن عملية استعادة النص الواضح من النص المشفر باستخدام مفتاح فك الشفرة تسمى عملية فك الشفرة Deciphering .

يعبر رياضياً عن عملية التشفير بالعلاقة

$$C = F_E (P , K)$$

حيث C النص المشفر، F_E خوارزمية التشفير، P النص الواضح، K مفتاح التشفير .

$$P = F_D (C , K)$$

حيثP النص الواضح،FDخوارزمية فك الشفرة،Cالنص المشفر،Kمفتاح فك الشفرة [Beker and Piper;1982]

يكون نظام التشفير مثالياً عندما تكون له القدرة على تشفير نص واضح بحيث تنتج أكثر من رسالة مفهومة عند فك شفرة الرسالة من قبل المعترض، ولا تتوفر للمعترض المعلومات الكافية ليقرر أي الرسائل المفهومة تم إرسالها عندها يقال عن هذا النظام الشفري نظام غير قابل للكسر [اسراء الوائلي؛ ٢٠٠٢][Dorth and Robling; 1982]

١-١-١ : نظام التشفير الجمعي :

هو واحد من ابسط أنواع معالجات أنظمة التشفير التقليدية التعويضية الذي يستخدم هجائية تشفير وحيدة لتشفير النص الواضح بأكمله والذي يعبر عنه رياضياً بالصيغة

$$C = (P + K) \text{ Mod } n$$

حيث C النص المشفر،P النص الواضح، K مفتاح التشفير السري، n فتمثل المعيار الحسابي. إن عدد مفاتيح التشفير المستخدمة في هذا النظام هو (n-1) .أما معالجة فك الشفرة فيكون حسب الصيغة الرياضية

$$P = (C + K) \text{ Mod } n$$ [Beker and Piper; 1982]

١-١-٢ : نظام التشفير الضربي :

هو أيضا نظام تشفير تقليدي تعويضي يستخدم هجائية تشفير وحيدة لتشفير النص الواضح بأكمله والذي يعبر عنه رياضياً بالصيغة

$$C = (P * K) \text{ Mod } n$$

حيث C النص المشفر، P النص الواضح، K مفتاح التشفير السري، n فتمثل المعيار الحسابي الذي يمثل عدد هجائية التشفير.ويمكن معالجة فك الشفرة باستخدام الصيغة الرياضية

$$P = (C * K^{-1}) \text{ Mod } n$$

حيث $K^{-1} = 1 \text{ Mod } n/k$ [Beker and Piper; 1982]

١-١-٣ : تشفير متعددات الحدود:

تستخدم أنظمة تشفير المفتاح السري (التشفير الانسيابي متعددات الحدود لأنها تعتبر الأساس في عمل مولدات المفتاح. يمكن تقسيم متعددات الحدود إلى ثلاثة أقسام هي:

أ- متعددات الحدود الأولية Primitive Polynomial

ب- متعددات الحدود غير القابلة للاختزال Irreducible Polynomials

ج- متعددات الحدود القابلة للاختزال Reducible Polynomials

إن أهمية متعددات الحدود الأولية على الحقل GF(2) هو الحصول على متتابعة بأكبر طـــول دورة (2^n-1) بمسجل إزاحة بطول n (عدد المراحل).

أي إن متعددة الحدود التي نولد متتابعة بأكبر طول دورة يجب أن تكون متعددة حدود أولية معاملاتها إما صفر أو واحد.

إن الشرط الضروري والكافي لمتعددة الحدود f(x) لتكون أولية هو أن تمتلك هذه المتعـددة أسـاً exponent يساوي (2^n-1) لأي مسجل بطول n [سلوى بعيوي؛٢٠٠٠]،[Golomb;1967] .

١-١-٤ : التشفير بطريقة نابساك:

تعتمد أنظمة التشفير من نوعية النابساك على اتجاهات رياضية مختلفة في عملية توليد المفتاح السـري والتـي كانت الأساس لأنواع مختلفة من أنظمة النابساك ومنها استخدام المتابعة المتصاعدة الذي قدم من قبل ماركـل-هيلمـان (١٩٧٨) وهي عبارة عن متجهة عناصره مجموعة أعداد موجبة تحقق خاصية أن يكون أي عدد من أعدادها اكبر من مجموع الأعداد التي سبقته [Odlzko; 1984]. ولكن واجه هذا النظام انتقادات عديدة بسبب كثافة متجهـة الواطئـة وكبر حجم المفتاح المعلن وكذلك لتعرضه للكسر من قبل العالم شامير، الذي قدم هجوماً ناجحاً على نظـام ماركـل-هيلمان وذلك في عام ١٩٨٠ [Adi and Zippel; 1980]، لذلك تم تطويره من الباحثان نفسهما وفي نفس عام كسره في اتجاهين هما :

الاتجاه الأول: باستخدام الضرب المعياري في بناء المفتاح المعلن والذي يعني (ضرب عناصـر المفتـاح المعلـن (متجهه نابساك) بعدد معين W واختزال الناتج لمعيار معين أخـر هـو Z علـى شـرط أن يكـون gcd(W,Z)=1 . علماً إن gcd هو القاسـم المشـترك الأعظـــــــم. اسـتخدام معكـوس العـــــدد W في عمليـــــة فـــــك الشفرة[Merkle and Hellman; 1978] .

الاتجاه الثاني: باستخدام التكرارات المتعددة والتي تعني (اختبار أكثر من زوج Z,W واسـتخدامها فـي عمليـة التشفير بشكل متعاقب في نظام ماركل-هيلمان المطور بالاعتماد على الاتجاه الأول [محمـد ابـراهيم؛ ٢٠٠٠] و[Dorthy and Robling; 1982] .

2-1: المنافذ

يمكنك اعتبار المنفذ كجهاز يربط المعالج Processor مع العالم الخارجي. فعن طريق هـذا المنفـذ يسـتقبل الإشارة من جهاز إدخال ويرسل إشارات أخرى إلى جهاز الإخراج.

تعرف المنافذ بواسطة عناوينها والتي تقع بين 0H-3ffH عنواناً مختلفاً. يجب أن لا ننسى إن هـذه العنـاوين مختلفة تماماً عن عناوين الذاكرة التقليدية، وهي لا تستعمل إلا مع تعليمتي IN و OUT المسـؤوليتين عـن معالجـة الإدخال والإخراج من هذه المنافذ بشكل مباشر.

نستطيع تحديد عنوان المنفذ بواسطة طريقتين مختلفتين استاتيكية و ديناميكية .

- **الاستاتيكية:** وعندها يكون عنوان المنفذ ضمن المجال ٠-٢٥٥ فقط وعلى شكل معامل مباشر.
- **ديناميكياً:** وعندها يوضع عنوان المنفذ ضمن المسجل DX مما يسمح باختيار العنوان ضمن المجال ٠-٦٥٥٣٥ على شكل معامل غير مباشر. تفيد هذه الطريقة بمعالجة مجموعة عناوين متسلسلة عن طريق زيادة أو نقصان قيمة المسجل DX.

نبين فيما يلي جدولاً لبعض عناوين المنافذ الشائعة الاستخدام [Able; 1998].

٠٢٠H- 023H	مسجلات حجب mask المقاطعة
٠40H- 043H	مؤقت/عداد timer/count
٠60H	الإدخال من لوحة المفاتيح
٠٦١H	مجهار Speaker الحاسوب
٢٠٠H- ٢٠FH	وحدة ضبط تحكم controller الألعاب
278H- 27FH	منفذ الطابعة المتوازي LPT3
2F8H- 2FFH	المنفذ التسلسلي COM2
٣٨٧H- 27FH	منفذ الطابعة المتوازي LPT2
3B0H- 3BBH	مكيف العرض المرئي وحيد اللون monochrome
٣BCH- 3BFH	منفذ الطابعة المتوازي LPT1
٣C0H- 3CFH	مكيف الرسوم البيانية المطورenhanced graphics
3D0H- 3DFH	مكيف الرسوم البيانية الملون
٣F٠H- 3F7H	ضبط تحكم القرص
٣F8H- 3FFH	المنفذ التسلسلي COM2

1-٢-١: الاتصال خلال المنفذ المتوازي القياسي

المنفذ المتوازي هو المنفذ الأكثر شيوعاً في ربط الحاسبات الشخصية. يسمح هذا المنفذ بمدخلات تصل 9 bits ومخرجات 12 bits في كل مره ولهذا يتطلب أدنى مستولى حماية خارجية لتنفيذ العديد من المهام البسيطة. يتألف هذا المنفذ من ٤ خطوط سيطرة، ٥ خطوط حالة، ٨ خطوط بيانات. عادةً ما يكون موقعه خلف الحاسبة كموصل من نوع D-25 pin إبرة مجوفة (female). كما يوجد أيضا موصل من نوع D-25 pin إبرة مستدقة (male) يمثل منفذ تتابعي RS-232 غير متوافق تماماً مع المنفذ المتوازي.

قيست المنافذ المتوازية الحديثة أول مره بـــ IEEE 1284 القياسي عام ١٩٩٤. ويعرف هذا المنفذ القياسي عملية هي:

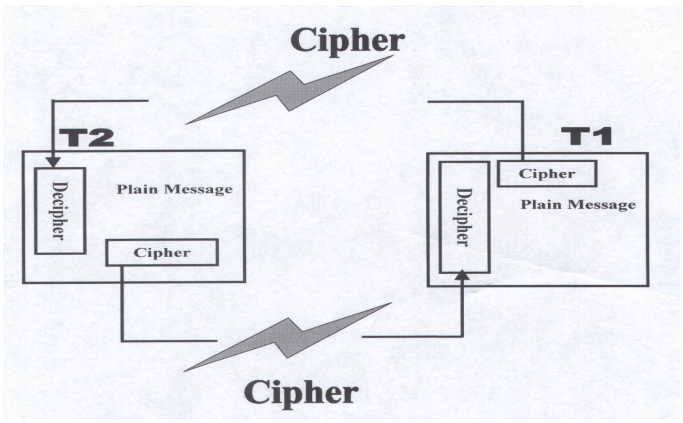
١- النمط التوافقي Compatibility Mode
٢- نمط Nibble Nibble Mode
٣- نمط بايت Byte Mode
٤- النمط المتوازي المحسن PP Mode (Enhanced Parallel Port)
٥- النمط الواسع الإمكانيات ECP Mode (Extended Capabilities Port)

تستخدم المنافذ الثلاثة الأولى الأجهزة hardware القياسية الموجودة على بطاقات المنفذ المتوازي القياسي. بينمـــا تتطلب النمطين الأخيرين أجهزة إضافية تمكنها من العمل بسرعة اكبر بحيث تبقى متوافقة مع المنفذ المتوازي القياسي.

يمكن للنمط التوافقي والمعروف بنمط Centronics إرسال بيانات بالاتجاه الأمامي فقط وبسرعة مثالية تصل إلـــى 50KB/S ويمكن للسرعة أن تزداد فتصل إلى 150KB/S. ولكي نتمكن من استقبال البيانات لابد من تغيير النمط إلى احد النمطين Nibble أو Byte . فبإمكان النمط Nibble إدخال 4bits بالاتجاه المعاكس (من الجهاز إلـــى الحاســـبة). النمط Byte يستخدم خاصية النقل باتجاهين (والموجودة على بعض البطاقات) لإدخال بايت (8bits) من البيانات فـــي الاتجاه المعاكس. يستخدم النمطين الأخيرين أجهزة إضافية لتوليد وتنظيم الاتصال باتجاهين[Peacock; 1998] .

٢- نظام تشفير البيانات الحية

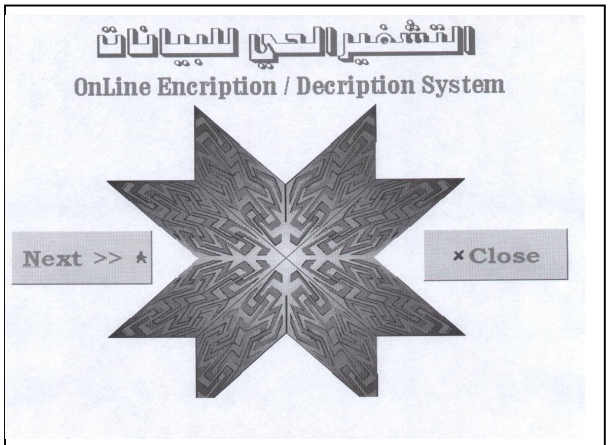
تم تصميم وبناء منظومة برمجية لتناقل وحماية البيانات المنقولة عبر قناة اتصال على طرفيها حاسبتين احدهما مرسلة والأخرى مستقبلة، حيث إن أي من الحاسبتين T1 أو T2 هي مرسلة والأخرى مستقبلة للبيانات وكما موضح في الشكل(١).



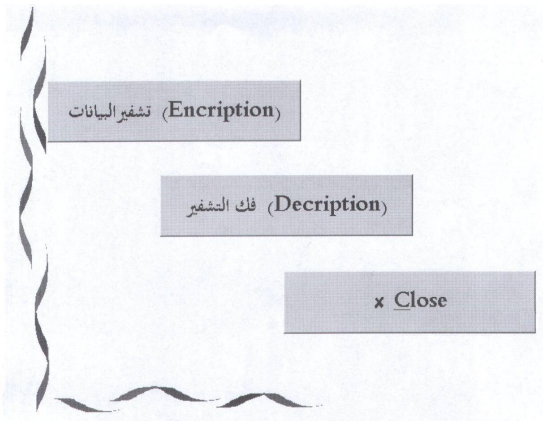
شكل (١) المخطط التوضيحي لنظام التشفير الحي للبيانات

إن كلا الحاسبتين المرسلة والمستقبلة تحوي على البرامجيات المنخفضة المستوى لاختيار المنفذ التي تم بنائها والتي اختير فيها المنفذ المتوازي بشكل ثابت لسهولة توفير الأدوات المادية اللازمة لتطبيقه بشكل عملي ولكن يمكن تغييره إلى أي نوع أخر وذلك لاستخدام الطريقة الديناميكية في اختيار نوع المنفذ بعد تحديد قيمة عنوانه.

كذلك تحوي كلا الحاسبتين على المنظومة البرمجية لحماية البيانات التي تحوي على الواجهة الرئيسية (شكل رقم ٢) الذي يحتوي على خيارين فقط هما الاختيار Close الذي يتم من خلاله غلق النظام والرجوع إلى نظام التشغيل، والاختيارNext الذي يسمح لك بالدخول للنظام والى نافذة اختيار التشفير وفك الشفرة (شكل رقم ٣) الذي يحتوي على ثلاث خيارات هي تشفير البيانات Encription والخيار فك الشفرة Decription وخيار Close .



شكل رقم (٢) الواجهة الرئيسية للمنظومة البرمجة لحماية البيانات.

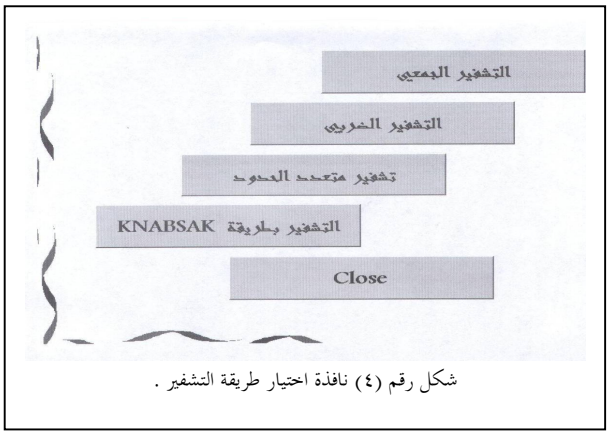


شكل رقم (٣) نافذة اختيار التشفير وفك الشفرة .

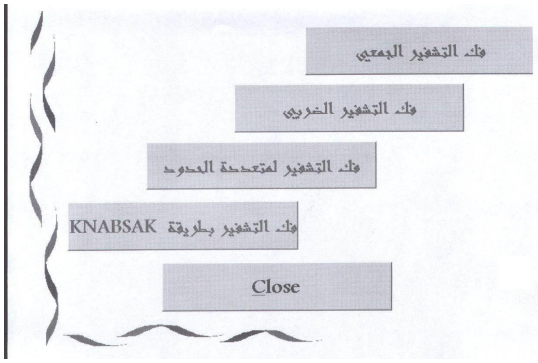
فإذا كنت تريد إرسال نص في هذه الحالة سوف تختار الخيار تشفير البيانات الذي يدخلك إلى نافذة اختيار طرق التشفير (شكل رقم ٤)، الذي يحتوي على خمس خيارات، الأربعة الأولى منها هي طرق التشفير التي تم تضمينها في هذا البحث وهي الاختيار الأول (التشفير الجمعي) والاختيار الثاني (التشفير الضربي) والاختيار الثالث (تشفير متعدد الحدود) والاختيار الرابع (التشفير بطريقة KNABSAK). أما الاختيار الخامس فهو (Close) للخروج من هذه النافذة والرجوع إلى نافذة التشفير وفك الشفرة.

أما إذا كنت تريد استقبال نص وفك شفرته في هذه الحالة سوف تحتاج الخيار فك الشفرة الذي ينقلك إلى نافذة اختيار طريقة فك التشفير (شكل رقم ٥) الذي يحتوي على خمسة خيارات أيضاً، الأربعة الأولى منها هي طرق فك

الشفرة لطرق التشفير المستعملة في النظام، وهي الاختيار الأول (فك التشفير الجمعي) والاختيار الثاني (فك التشفير الصفري) والاختيار الثالث (فك التشفير متعدد الحدود) والاختيار الرابع (فك التشفير بطريقةKNABSAK) أما الاختيار الخامس فهو لغلق النافذة والرجوع إلى النافذة السابقة.



شكل رقم (٤) نافذة اختيار طريقة التشفير .



شكل رقم (٥) نافذة اختيار طريقة فك التشفير .

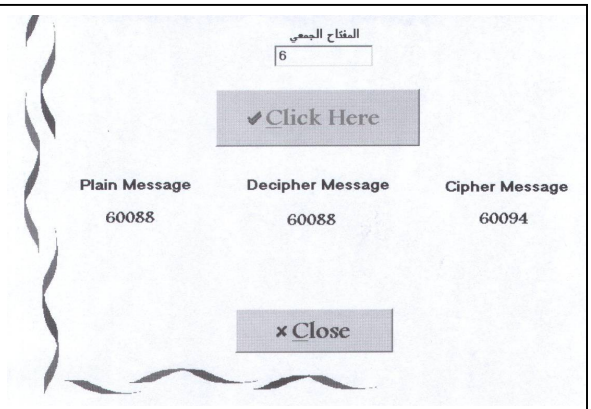
التشفير الجمعي :

يتناول التشفير الجمعي إضافة مقدار معين (المفتاح الجمعي) يتم إدخاله من استمارة الإدخال (شكل رقم ٦) ويضاف هذا المقدار إلى قيمة النموذج الأصلي (النص الواضح) لكي يأخذ قيمة أخرى غير القيمة الأصلية وبهذا تحول النص الواضح بعد التشفير إلى نص أخر(النص المشفر).

هذا النص المعالج والناتج يحول بشكل مباشر إلى المنفذ المختار (المنفذ المتوازي) عن طريق منظومة البرمجة التي بنائها ثم عبر قناة الاتصال إلى الحاسبة المستقبلة الموجودة في الطرف الأخر، ليتم قراءته (النص المشفر) من المنفذ المربوط على قناة الاتصال (المنفذ المتوازي).

بعد ذلك يتم عملية فك الشفرة من خلال إدخال قيمة مفتاح فك الشفرة في استمارة إدخال فك الشفرة (شكل رقم ٧) المعروف مسبقاً لديهم ليتم استخراج النص الأصلي (النص الواضح).

شكل رقم (٦) استمارة الإدخال لتشفير نظام التشفير الجمعي



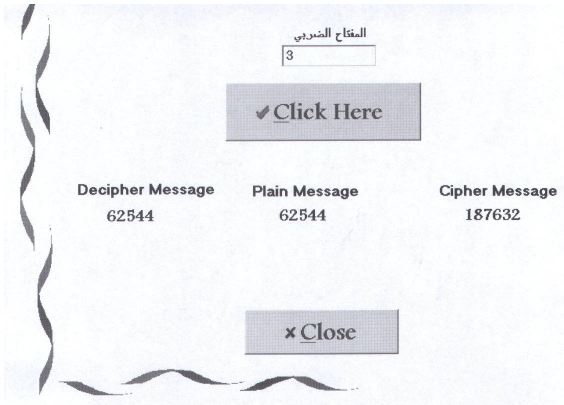
شكل رقم (٧) استمارة إدخال فك الشفرة لنظام التشفير الجمعي

التشفير الضربي :

كما في التشفير الجمعي فان التشفير الضربي يعتمد على ضرب مقدار معين (المفتاح الضربي) يتم إدخاله من استمارة الإدخال (شكل رقم ٨) في مقدار قيمة النموذج الأصلي (النص الواضح) لكي يأخذ قيمة أخرى غير القيمة الأصلية، وبهذا يتحول النص الواضح بعد التشفير إلى نص أخر(النص المشفر). الذي يحول بشكل مباشر إلى المنفذ المختار (المنفذ المتوازي)، ثم عبر قناة الاتصال إلى الحاسبة المستقبلة الموجودة في الطرف الأخر ليتم قراءته (النص

المشفر) من المنفذ المربوط على قناة الاتصال (المنفذ المتوازي). بعد ذلك يتم عملية فك الشفرة من خلال إدخال قيمة مفتاح فك الشفرة في استمارة إدخال فك الشفرة (شكل رقم ٩) المعروف مسبقاً لديهم ليتم استخراج النص الأصلي (النص الواضح).

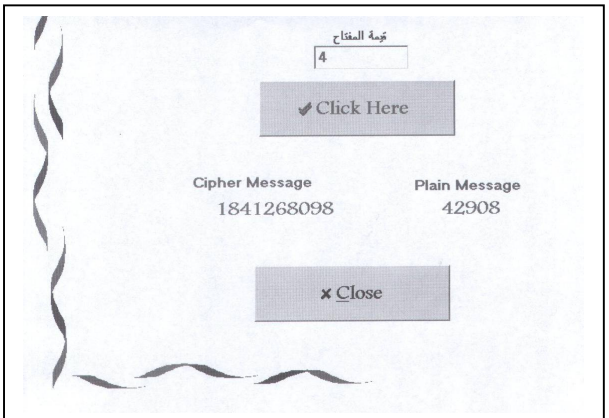
شكل رقم (٨) استمارة الإدخال لتشفير نظام التشفير الضربي



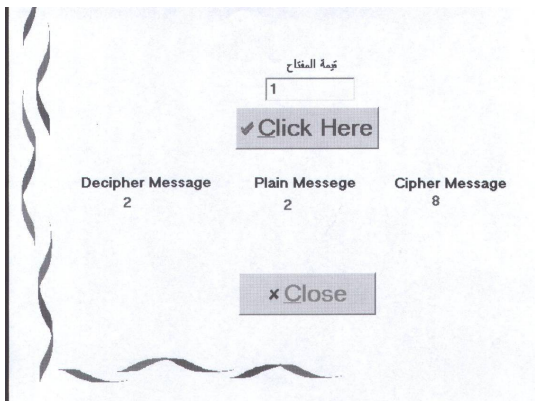
شكل رقم (٩) استمارة إدخال فك الشفرة لنظام التشفير الضربي

التشفير بطريقة متعددات الحدود

تعتبر هذه الطريقة أكثر تعقيداً من الطريقتين السابقتين لكون النص الواضح يمكن أن يخضع لعمليات رياضية وكذلك تضاف علية قيم ثابتة ليدخل على أكثر من حد (شكل رقم ١٠) خلاف الطريقتين السابقتين التي تعتمدان على حد واحد ، وبذلك يكون النص الواضح قد اختفيت معالمه تماماً ويصعب استرجاعه من قبل محلل الشفرة. تم عملية فك الشفرة لمتعددة الحدود كما موضح في (شكل رقم ١١).



شكل رقم (١٠) استمارة الإدخال لتشفير طريقة متعددة الحدود



شكل رقم (١١) استمارة إدخال فك الشفرة لطريقة متعددة الحدود

التشفير بطريقة نابساك

تعتبر طريقة ماركل–هيلمان إحدى الطرق المهمة من أنظمة تشفير المفتاح المعلن نوع نابساك، ويعتمد على وضع أنظمة تشفير ذات أبعاد رياضية متعددة لإخفاء قيمة المفتاح السري . استخدام النوع التقليدي هنا في التشفير حيث تم إدخال قيم متسلسلتي النموذج الأصلي (النص الواضح) والمفتاح السري لإخراج النص المشفر(شكل رقم ١٢) .

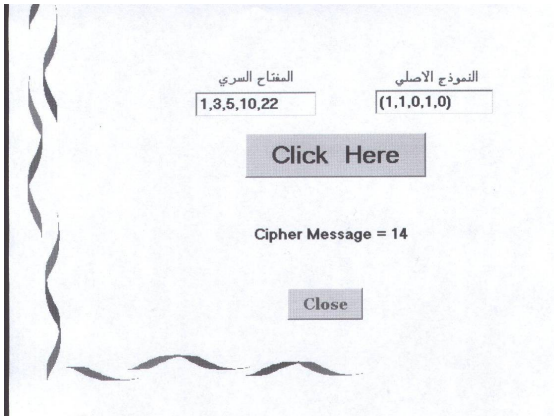
إن الخطوات الأساسية لتشفير هذا النظام يمكن إيجازها بالخطوات الآتية:–

١–اختيار متتابعة من الأعداد العشوائية لتحقيق شرط المتتابعة الآتية لكي تمثل عناصر المفتاح السري.

2- تحويل الرسالة إلى التمثيل الثنائي $X=(x_1,x_2, \ldots ,x_n)$. حيث تمثل عناصر المتجه X ثنائيات النص الواضح.

٣- عملية التشفير تتناول مزج متسلسلة النص الواضح مضروباً بمتسلسلة المفتاح السري.

أما في عملية فك الشفرة لهذا النظام فيتم إدخال قيم متسلسلة المفتاح السري وقيم النص المشفر لإنتاج النص الواضح (شكل رقم ١٣).



شكل رقم (١٢) استمارة الإدخال لنظام التشفير بطريقة النابساك

شكل رقم (١٣) استمارة الإدخال لفك الشفرة بطريقة النابساك

٣-النتائج

١- أن المنظومة البرمجية التي تم تصميمها وبنائها هي بيئة صديقة للمستخدم وسهلة الاستخدام.

٢- بناء برنامج بلغة التجميع تتعامل مع منافذ الحاسبة المختلفة التي يمكن تبديل عناوينها باستخدام الطريقة الديناميكية.

٣- تم تصميم وبناء منظومة لتشفير هذه البيانات باستخدام عدة طرق وقابلية التبديل العشوائي المتفق عليه لكي يصعب على المتجسس او المتلصص على البيانات من متابعة طريقة التشفير وتحديدها ومهاجمتها.

٤- سرعة المعالجة للمنظومة تعتمد على طريقة التشفير التي تم استخدامها ودرجة تعقيدها ويجب أن لا يكون الموديل الرياضي للتشفير معقد لكي تكون فترة الحماية للبيانات المنقولة هي قصيرة جداً بحيث لا يضيف وقت تأخيري على عملية الإرسال والاستقبال.

٥- أن استخدام منظومة الحاسبة إضافة تسهيلات أخرى لناقل البيانات السرية هي عملية التوثيق والتخزين العالية السرعة وكذلك الحجم الهائل لخزن البيانات.

٤-المقترحات والأعمال المستقبلية:

١- بناء برنامج تهيئة للمنظومة يعمل في بداية تشغيلها يتم فيها تحديد المنافذ المستخدمة للاتصال والطريقة التشفير المراد استخدامها.

٢- يمكن تقوية المنظومة باستخدام طرق تشفير أخرى بتعقيدات مختلفة وبعدد اكبر لكي يصعب على المتجسس تحددها ومهاجمتها.

٣- لقد تم اختيار المنفذ المتوازي لتجريب النظام على طرفي قناة الاتصال ويمكن اختيار أي منفذ أخر مثل modem وربطها بالشبكة الدولية Internet .

٦- المصادر:

[اسراء الوائلي؛ ٢٠٠٢] اسراء عدنان الوائلي؛ " **تصميم ومحاكاة نظام لمعالجة الصور(التشفير والترميز)**" ، رسالة ماجستير ؛ جامعة بابل-كلية العلوم؛ ٢٠٠٢.

[دايفس شبمان؛ ١٩٩٩] دايفس شبمان ؛ " **علم نفسك Visual C^{++}6 في ٢١ يوماً** "؛ الدار العربية للعلـــوم، الطبعـــة الاولى؛ ١٩٩٩.

[سلوى بعيوي؛٢٠٠٠] سلوى شاكر بعيوي؛ "**مقارنة بعض طرائق انظمة التشفير الانسيابي في تطبيق تقنية تحليـــل الشفرة بمبدأ النص الواضح-المعرف**"؛ رسالة ماجستير؛ جامعة بابل-كلية العلوم ؛٢٠٠٠.

[محمد ابراهيم؛ ٢٠٠٠] محمد خليل ابراهيم؛ " **تحليل وتقويم انظمة تشفير المفتاح المعلـــن مـــن نـــوع النابســـاك باستخدام الشبكات العصبية الاصطناعية**"، رسالة ماجستير، جامعة بابل-كلية العلوم؛٢٠٠٠.

[Able; 1998] Peter Able; **"IBM PC Assembly Language and Programming"**; Prentice-Hall International Inc.; Fourth Edition; 1998.

[Adi and Zippel; 1980] Adi S. and Richard E. Zippel; **"On the Security of th Merkle-Hellman Cryptographic Scheme"**; IEEE Trans. Inform. Theory; Vol. IT-26; No. 2; 1980.

[Beker and Piper; 1982] H. Beker and F. Piper; **"Cipher System (The Protection of Communications)"**; Printed and Bound in Great Britain Ltp.; Edinburgh and London;1982.

[Deitel and Deitel; 1998] H. M. Deitel and P. J. Deitel; **"C^{++} How to Program"**; Prentice-Hall International Inc.; Second Edition; New Jersey; 1998.

[Dorthy and Robling; 1982] Dorthy E. and Robling D.; **"Cryptography and Data Security"** ; Addison-Weasly publishing Company; Inc.; 1982.

[Golomb ;1967] Golomb S. W.; "**Shift Register Sequences**"; Holden-Day; 1967.

[Merkle and Hellman; 1978] Relphe C. Merkle and Martin E. Hellman; **"Hiding Information and Signatures in trapdoor knapsacks"**; IEEE trars. Inform. Theory; vol. IT-24; No. 5; 1978.

[Odlzko; 1984] Odlzko A.; "**Discreate Logarithm in Finite Field and Their Cryptographic Significance"**; Lecture notes in Computer Security 209; Eurocrypt 84; At & T Bell Laboratories; Morrey Hill; New Jersey 07974; 1984.

[Peacock; 1998] Craig Peacock; **"Interfacing the Standard Parallel Port",** www.senet.com.au/~cpeacock; 1998.

[Tarish; 2000] A. H. Tarish; **"Digital Image Cryptography"**; M. Sc. Thesis, Technology University; 2000.