Toward increasing Security and Role of Encryption Key for Computer based Encryption System

Asst. Lecturer Firas abdul Elah abdul Kareem

Computer Technologies Eng. Dept.
Al-Mansour University College

Abstract

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables us to store or transmit sensitive information across insecure channel (like Internet), by making it unreadable except to intended recipient .A key is a value that works with a cryptographic algorithm to produce a specific cipher text .The bigger the key, the more security that we will gain. In the case when encryption system was executed on personal computer connected to the net or on the net server itself, the encrypted data security depends on:

- **The strength of the cryptographic algorithm.**
- **The secrecy of key storage method and its immunity against direct physical attacks, or attacks from net.**

There are many traditional ways for storing encryption keys (floppy disk, PC hard drive ,paper in our pocket ,paper stored in locked cabinet … ,etc) .In this research there will be a try to increase the encrypted data security through two directions ,first by increasing the security of key storage by introducing a untraditional hardware physical module for that purpose ,and the second by increasing the role of encryption key into encryption algorithm executed on computer through :

- **Introduce a new way for entity (user) authentication.**
- **Design of external hardware module attached to PC parallel port to improve encryption key storage security and Role.**
- **Gaining improvement in the security level for PC based encryption system (or any other microprocessor based) encryption system.**

1 Introduction:

Encryption is a way of protecting data against unauthorized use .Several techniques have been used throughout the years to protect data against enemies who would misuse the information .Thousands of years ago, the main use of encryption was to protect data during war [1,2].

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables Us to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient .Cryptography basic objectives are (Confidentiality ,Data integrity ,Authentication ,Non-repudiation) [2]. The Cryptography objective of Confidentiality is a service used to keep the content of information secure from all but those authorized to have it is strongly related to this research .This research will deal with private key cryptography .The security of many cryptographic systems depends upon the generation of unpredictable quantities [1,2] .To run the cipher machine ,we need to stick a key in it .We can stuff plaintext in one side and get cipher text out the other side .We can run the cipher in machine in reverse to convert cipher text to plaintext [2,4] .In practice, the cipher is a mathematical formula .A key is just a special number ,or a few special numbers, that are used in the formula .There are many ways to store keys .We could just write the key's values out to a file ,or we might add a header with additional information about the key .If our file system isn't protected from intruder ,we have to be careful about writing private keys to file.

One solution is to encrypt the keys themselves, perhaps with a pass word, before writing them out. Another solution for storing private keys is to put them on removable media, like floppy disks or smart cards [1].

To protect our private key we must be sure (as much as we can) that our private key is kept secure away from third entity [1] ,and change the form of storing keys (example use encryption for keys).

This research objective ,is to design ,implement and evaluate a hardware security module (HSM) attached to PC parallel port that serve protecting our private key carefully (as much as we can) by being sure that our private key is kept secure away from third entity through changing the media and form of storing our private keys ,by introducing a new way of physical protection of our private key ,to prevent physical direct access of enemy to our key .Also new ideas was designed and analyzed to produce larger and more effective role for our key into the Encryption Algorithm.

2 Cryptographic Algorithm and private key cryptography:

A cryptographic algorithm is a mathematical function used in the encryption and decryption process in combination with a key to encrypt the plaintext; the security of cipher system depends on the strength of the cryptographic algorithm and the secrecy of the key [1,2,3]. Private key cryptography or (secret key cryptography), is the kind of cryptography used in earlier days .The term private key is used because this technique implies that both the sender and the receiver of the message have a same key that must be kept private (figure 1).

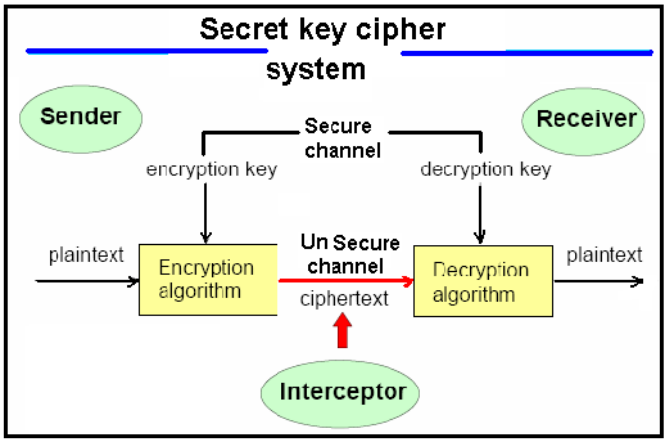

Figure 1 (Secret key system)

2.1 Linear Feedback Shift Registers (LFSRs):

Linear Feedback Shift Registers (LFSRs) in binary form are the workhorse circuits in present day electronic cipher systems [1].

LFSRs appear in virtually any communication and storage device .They play a important role in generating sequences, error-correction and error detection and in scrambling and descrambling applications .

We may find them in mobile phones , CD and DVD players ,modems and almost any coding application .

Assuming a LFSR with length (L) stages and with connection polynomial C(D) defined as shown in (figure 2) [1] ,and If C(D) is irreducible ,then output sequence period is ($2^L - 1$) .The LFSR output sequence have large period and good statistical properties.

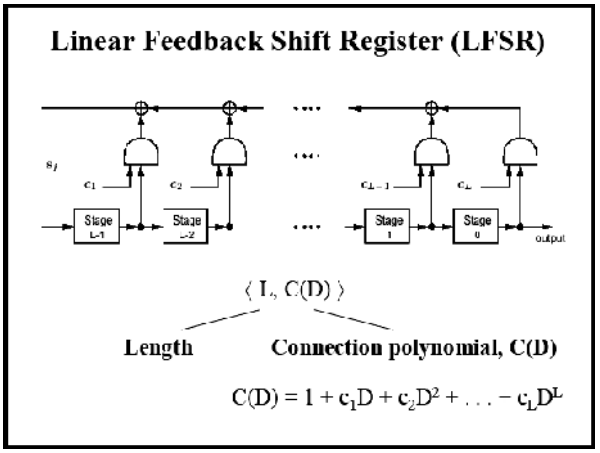

Figure 2 (LFSR scheme)

2.2 Permutations:

Functions which are often used in various cryptographic algorithms [1,2]. Let S be a finite set of elements.

A *(permutation P)* defined on set (S) is a function from set(S) to itself, i.e. (P : S → S) .For example let S ={1,2,3,4,5} ,with P defined on (S) as following : P(1) =3 , P(2) =5 , P(3) =4 , P(4) =2 , P(5) =1 .

A permutation can be described in various ways .It can be displayed as above or as an array as following:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

2.3 Using PC parallel port for data transfer:

The Parallel Port is the most commonly used port for interfacing homemade projects. This port will allow input of up to 9 bits or output of 12 bits at any one given time, thus requiring minimal external circuitry to implement many tasks. The port is composed of 4 control lines, 5 status lines and 8 data lines, found commonly on the PC back as a D-Type 25 Pin female connector (figure 3) .The driver software that comes with the card responsible for determining the used ports addresses [5] .

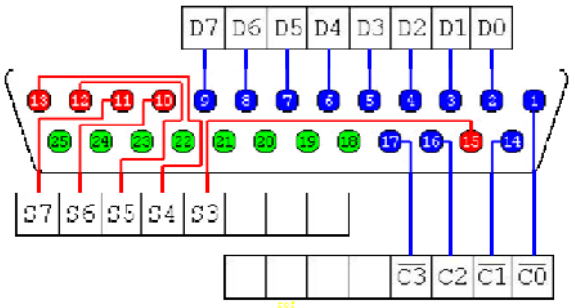

Figure 3 (25-way Female D-Type Connector)

The Parallel Port could be used to Input 8 Bits .We can input a maximum of 9 bits at any one given time, by using the 5 input lines of the Status Port and the 4 inputs (open collector) lines of the Control Port, as shown in the following figure [5]:

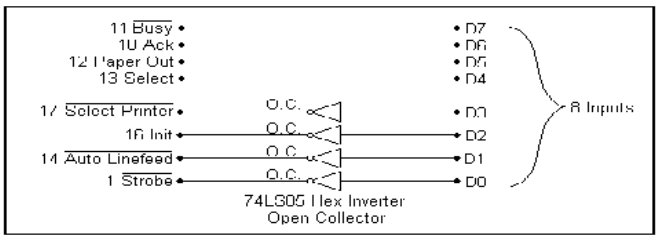

Figure 4 (using parallel port to input 8 bits)

The parallel port allows the output of 12 bits at any one given time. The 12 bits make use of 8 bits from (data port register) of Standard Parallel Port (SSP), plus 4 bits from (control register) they are (Auto-Linefeed, initialize, Select-Printer/ Select-in, Strobe).

3 Suggested Cryptographic schemes:

In this part, a practical attempt to increase the security of cryptographic key storage and role of key in the cryptographic algorithm was done, depending on the fact that (Keeping the key as secret is difficult, but also guarding all information regarding the Cryptographic Algorithm is much harder) [1,2,3]. What was believed as last defending line, which is the cryptographic key was gained more security and role in the cryptographic algorithm, through design and evaluate an external Hardware Security Modules (HSM) attached to PC parallel port, to increase the key role and the security of the key management functions (Generation, Storage, Activation, Establishment) which worked together with cryptographic algorithm. The keys will be stored inside a tamper-resistant hardware module. Three cryptographic schemes are designed and evaluated as follows.

3.1 First scheme: (Look-up table's usage to increase the period of LFSR based key stream generator):

Lookup table is any stored binary data in (EPROM) or memory and is widely used in digital circuits for implementing Boolean functions by storing digital variables of Boolean function in memory, and by proper addressing of this memory, the memory digital output will be used to synthesize the required Boolean function. In the first proposed HSM, a lookup table will be used to store and then select one primitive polynomial (from many) as key for LFSR based key stream generator ,as shown in the following figure:

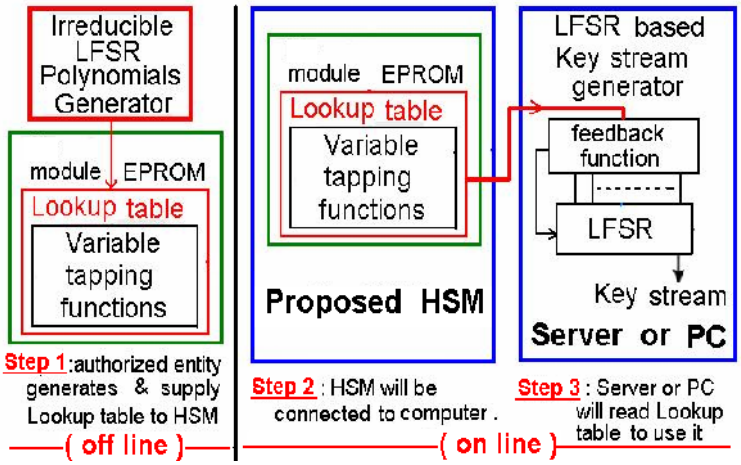

Figure 5 (first proposed scheme)

As shown in (figure 5), the cryptographic algorithm was running on the computer (Server or normal PC) and needs to read the tapping factors from the proposed HSM to synthesize a LFSR based key stream generator. The tapping factors are stored as secret key in the proposed HSM which is attached to computer parallel port .If many tapping cases are stored, the resultant will be an extended period LFSR based key stream generator. As an example ,let we have a LFSR key stream generator of 9 bits length for shift register as shown in figure 6 [1]:

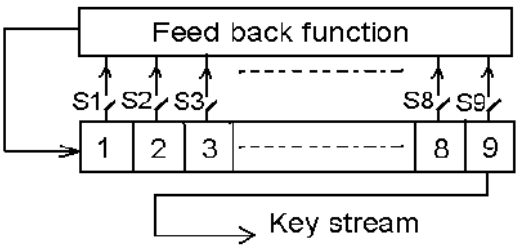

Figure 6 (LFSR based key stream generator)

S1, S2… S8,S9 are binary value switches, such that when a certain stage of order (n) of LFSR is participated in feedback function then (Sn = 1), otherwise (Sn =0).

What will be stored in the proposed HSM at factory stage ,are 9 bits for each possible irreducible polynomials that represent the participated LFSR stages in the feedback function that will be synthesized as shown in the following figure [1]:

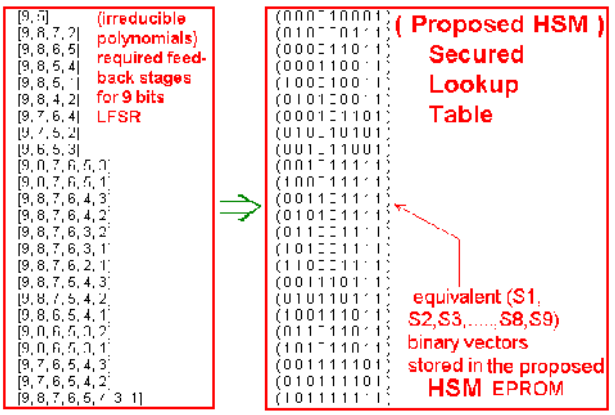

Figure 7 (1st scheme secured look up table)

The server or PC that have to run the cryptographic system for data protection, will have to read binary feedback constant vector from the proposed HSM .For 9 bits LFSR ,the number of(irreducible polynomials) ,that gives maximum period of ($2^9 - 1$) as shown in figure 7.

3.1.1 Analyzing the power points of the proposed extended period LFSR key stream generator:

- **There will be difficult task for the cryptanalyst and provide more security was provided, because the tapping polynomials will be changed in random manner.**
- **Even if the current tap is broken the attacker will not know which will be the next tapping function.**
- **The initialization tapping based on the key provided by the user.**
- **When the complete period of output sequence Is finished ,the connection polynomial is reset with another one of those stored in our module ,and a different sequence is obtained .**

Extended period of our scheme = total number of existing irreducible polynomials × ($2^{n} - 1$))

- **for our example : extended period = 24 X ($2^{9} - 1$)) = 12264 bits.**

- **By updating of HSM EPROM data (as a key change) ,we can get different order for maximum period irreducible feedback polynomials**

3.1.2 The advantages gained from 1st proposed scheme:

1. **The most important part of encryption algorithm (tapping vectors) is stored outside computer.**
2. **The security is increased because the tapping polynomials will be selected pseudorandom way, so even if the current tap is broken the attacker will not know which will be the next tapping.**
3. **Tapping functions are generated at initialization stage, resulted in high execution speed.**
4. **The complete output period is extended.**
5. **Increasing the LFSR length will increase irreducible polynomials tapping functions number too, means harder job for attacker.**
6. **User Key role is increased and more activated.**
7. **The output still has good statistical properties since it consists of complete periods of LFSR.**

3.2 Second scheme: (Look-up tables usage to increase the user key storage security):

- **The proposed HSM and its lookup table can be used to increase the security of key storage as shown in the following figure :**

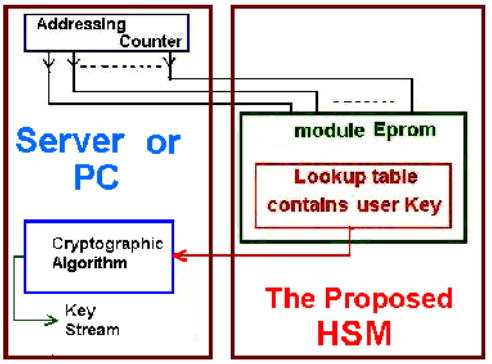

Figure 8 (Second proposed scheme)

- The keys are generated and stored before our PC or server is connected to network.
- The proposed HSM is connected to computer parallel port for key retrieving.
- When key is retrieved, HSM could be disconnected from computer.

3.2.1 The advantages taken from 2nd scheme:

1. Important part of encryption algorithm (User keys) are stored outside computer .All physical threats [1, 2,3] (such as copying ,modifying) will not be reflected to user key .
2. The security is increased since keys could be changed more frequently and easily by changing proposed HSM with updated one.
3. User Key role is increased and more activated.
4. Key materials can be better protected from network attacks than if they were running inside a general purpose server, since Key materials are stored on the HSM, not the server .Virtually it is impossible for HSM to be attacked over a network.

3.3 Third scheme: (Lookup tables usage to increase Security and Role of Permutation boxes):

- Permutation boxes are used in the 3rd scheme to add an area for user finishing touches to change the behavior of encryption algorithms in a way that increase the user role to achieve more security.

- Data input to permutation box are permuted in its output according to user selecting switches as shown in following figure that takes an example of permutation box of size 4:

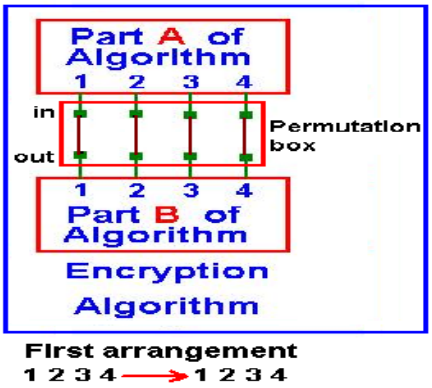

Figure 9 (3rd proposed scheme)

- Figure 9 shows (as example) the case when user prefers no data permutation in data transferring from part A to part B.
- Figure 10 shows another two arrangements with different user setting of permutation box.

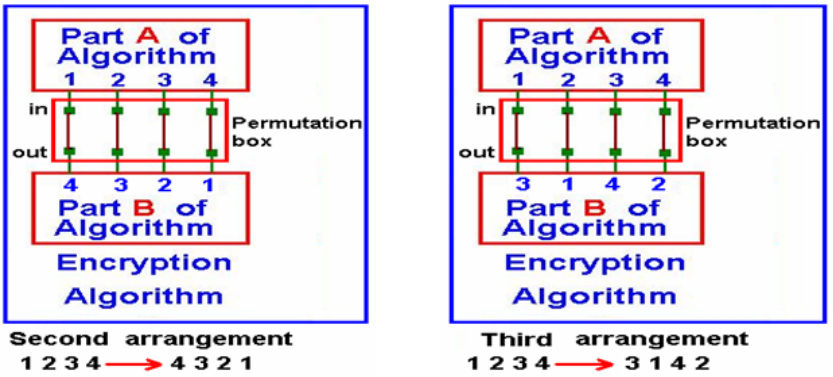

Figure 10 (different user permutation box setting)

3.3.1 Security analysis for scheme mentioned in (figure 10):

- since there are (n!) ways to arrange (n) objects into groups of size (n) at a time ,then for our scheme (when n =4):
  Number of all possible permutations = (4!) = 24.

- Thus, even if the encryption algorithm is known, the attacker of algorithm must have to work on (attack) (24) different arrangements of encryption algorithm rather than one arrangement when there is no permutation box is used.

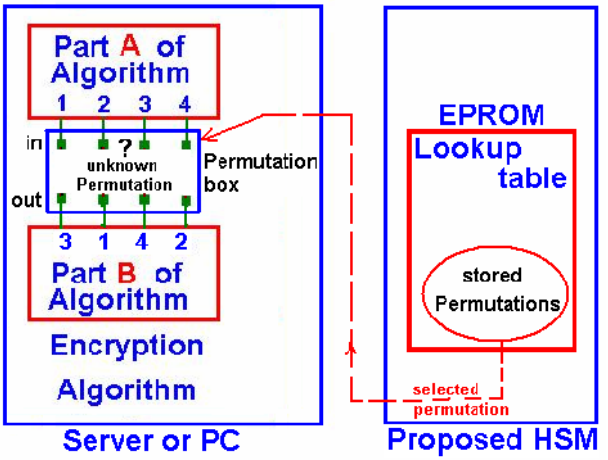

Figure 11 (Server /PC) connection with proposed HSM

- In (figure 11), the procedure for proposed scheme for permutation box of size (n) is to store the (n!) permutations in the EPROM of HSM which is connected to PC or server parallel port .One permutation is used as arrangement for encryption algorithm.
- Expired Permutation has to be replaced with new retrieved from HSM to get arrangement which is unknown for attacker.
- Available permutation number when: n=4 → n! = 24
  n=5 → n! = 120 n=6 → n! = 720

  n=7 → n! = 5040

  n=8 → n! = 40320 ….. Etc. Thus, we conclude that as (n) increased linearly, the number of permutations is increased in non linear way.

3.3.2 Permutation Box Logic for our example (n = 4):

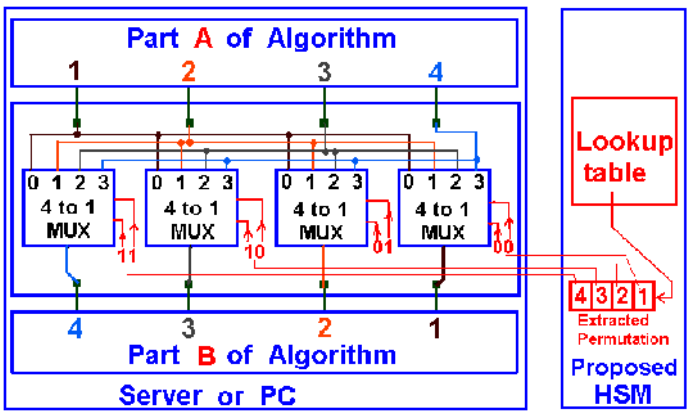

Figure 12 (permutation box Logic)

The above figure (12) example take a permutation value of (4 3 2 1) for demonstration purpose of required logic for permutation action.

3.4 Hardware interface requirements of proposed schemes:

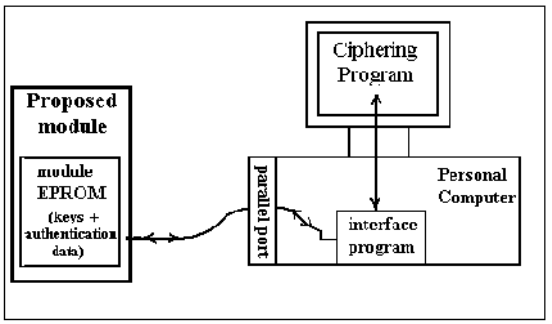

Figure13 HSM/PC interface

Referring to (figure 13), the following are some features:

1. **PC parallel port allows either input of up to 9 bits or the output of 12 bits at any one given time.**
2. **The output of the Parallel Port is normally TTL logic levels.**
3. **Most Parallel Ports can sink and source around 12mA, however it is better to use a buffer, so the least current is drawn from the Parallel Port.**
4. **In order to make our module work correctly on many Printer Ports as possible, we can use an external internal pull-up resistor (4.7k) for input and output lines.**
5. **Buffers and external pull up resistors mentioned in points 3, 4 (above) are parts of interface circuit, as shown in (figure 14).**

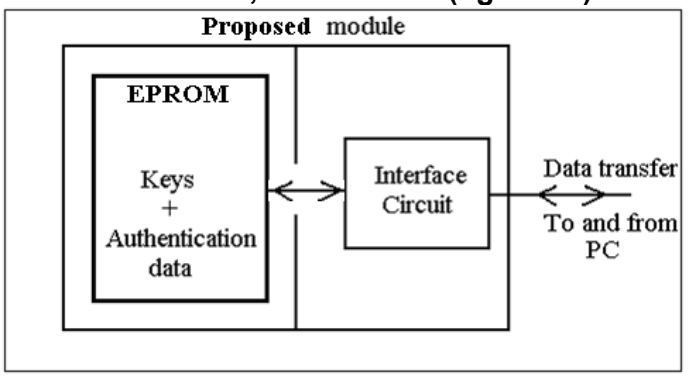

Figure 14 (proposed module interface scheme)

3.5 Ciphering and Interface programs interaction steps:-

1. **Run the interface program to initialize two ways communication with proposed HSM, to supply selected EPROM addresses.**
2. **For these addresses, interface program will read EPROM contents to store them in array, for later use by ciphering program.**
3. **Ciphering program will check the authentication data to decide whether the user is authorized or not .If authorized, the ciphering program will enter in ciphering or deciphering phases according to our need to send or receive messages respectively.**

4. Concluded advantages of proposed (HSM) Schemes:

1) **More space was gained for cryptographic algorithm keys.**
2) **More role value was gained for keys into cryptographic action.**
3) **Security key functions, are performed in hardware instead of software that means, key materials can be better protected from network attacks when they were running inside a general purpose server, since they are stored on the proposed HSM, not the server, and they do not run under operating system ,therefore virtually impossible to attack over a network.**
4) **Security functions regarding cryptographic keys when performed in hardware instead of software enable us to gain better protection from physical attacks such as copying ,modifying …etc .**
5) **Proposed HSM can be custom designed, securely sealed, to produce more ambiguity for intruder.**
6) **Hardware may be less susceptible to system failures and corruptions, such as viruses.**
7) **Proposed HSM could be carried with us without inducing suspicion, since it looks like any electronic card for any general purpose.**
8) **The storing media is different from computer that has our private encrypted messages files will offer more security, and add more immunity against network attacks according to what is advised in [4].**
9) **Even if the proposed HSM falls on the intruder hands ,it will be not useful for him since he neither know hardware details of this module nor the software required to make use of data stored inside it.**

5 Future works:-

1. **As number of output bits that could be supplied buy parallel port at any time is 12 bits, then max HSM EPROM size that could be used in the proposed HSM modules is 4096 bytes. If more size is needed an external hardware circuitry could be used with some required modifications in the interface program.**
2. **In IBM system, the addresses (300 h) to (31F h) are reserved for prototype cards .Thus a general purpose INPUT/OUTPUT cards could be design to have an interface hardware between the proposed HSM and the computer rather than using printer port .The connection between proposed HSM and general INPUT/OUTPUT card could be performed using an extension cable .Working on general purpose INPUT/OUTPUT card more EPROM address space and more size for data transferred could be achieved.**
3. **Working on adding encryption for the proposed HSM contents to prevent direct access to HSM keys.**

6. References

1. **Cipher systems: Henry Beker and Fred Piper .Copy right by Northwood Publications 1982.**
2. **Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone. Copy right 1997 by CRC Press, Inc**
3. **Java Cryptography Jonathan B. Knudsen .First Edition May 1998 by O REILLY.**
4. **Hardware Security Modules : Where Businesses Puts Its Trust ,an AEP Systems White Paper January 2003**
5. **Programming the Parallel port .Interfacing the PC for Data Acquisition and Process Control .By Dhananjay V. Gadre . Copyright © 1998 by Miller Freeman, Inc.**

نحو أكتساب زيادة في أمنية ودور مفاتيح التشفير لنظام تشفير حاسوبي

م.م. فراس عبد الأله عبد الكريم
قسم هندسة تقنيات الحاسوب
كلية المنصور الجامعة

المستخلص

علم التشفير هو علم أستخدام قواعد رياضية محددة لتشفير وأزالة التشفير للمعلومات المهمة لتمكيننا من خزن المعلومات الحساسة أو نقلها عبر شبكات أتصال غير سرية (مثل الأنترنيت) بشكل لايمكن الأستفادة منه ألا للمستلم المقصود.

مفتاح التشفير هو القيمة التي ستعمل مع خوارزمية التشفير لأنتاج النص المشفر ، وكلما أزداد طول مفتاح التشفير كلما كان ممكنا لنا الحصول سرية أكبر للنص المشفر.

في حالة كون نظام التشفير مطبق على حاسبة شخصية مرتبطة بشبكة الأنترنيت أو على الحاسبة المركزية الحاوية على قاعدة بيانات مهمة والمرتبطة بالشبكة فأن سرية المعلومات المشفرة تعتمد كليا على تحقيق الهدفين التاليين معا:

- قوة ومنعة خوارزمية التشفير.
- سرية أسلوب خزن مفاتيح التشفير ومناعته ضد أساليب الهجوم الفيزيائية المباشرة أو القادمة عن طريق شبكة الأنترنيت.

في هذا البحث ستتم محاولة تحقيق سرية أكبر للمعلومات المشفرة من خلال أتجاهين ، الأول تحقيق مستوى أمنية أعلى لعملية خزن المفاتيح لنظام تشفير مطبق على الحاسوب عن طريق أقتراح تركيب فيزيائي مادي غير تقليدي لخزن المفاتيح ،والثاني بأتجاه زيادة دور مفاتيح التشفير في خوارزمية التشفير وذلك عن طريق:

- تقديم وتصميم وتنفيذ وتقويم أداء وحدة مادية خارجية ترتبط بالمنفذ المتوازي للحاسوب لرفع مستوى السرية للتعامل مع عملية خزن مفاتيح التشفير.
- الوصول الى مستويات أمنية أعلى لنظام التشفير الحاسوبي أو أي نظام تشفير أخر يعتمد على ا**لمعالج** الدقيق كوحدة بناء أساسية.