Proposal New Approach for Blowfish Algorithm by Using Random Key Generator

Israa Tahseen[1]and Shatha Habeeb[2]
University of Technology, Computer Sciences Department
[1]Israa80atar@yahoo.com, [2]ShathaHabeeb@yahoo.com

Abstract

There are three basic encryption methods: hashing, symmetric cryptography, and asymmetric cryptography. Each of these encryption methods has their own uses, advantages, and disadvantages. All the three of these encryption methods use cryptography or the science of scrambling data. Although there are several pieces to an encryption process, the two main pieces are the algorithms and the keys. Blowfish, a symmetric block cipher and a Feistel network which follows simple Enciphering and Deciphering functions of 16 times each. The strength of the Blowfish algorithm relies on its sub-key generation and its basic confusion and diffusion based design. The proposed method are generate key drawn from parts of the image and by the size of key used with Blowfish.

Key word: Blowfish, symmetric, key, encryption, ciphertext.

المستخلص

طرق التشفير الأساسية ثلاثة: التجزئة والتشفير المتناظر والتشفير غير المتناظر. كل من هذه الأساليب للتشفير لها استخدامات خاصة ومزايا وعيوب. كل هذه الأساليب تتضمن استخدام التشفي أو علم هرولة البيانات. على الرغم من أن يكون هناك عدة اجزاء لعملية التشفير، والاجزاء الرئيسية هي الخوارزميات والمفاتيح blowfish. تشفيركتلة متماثل وشبكة تتبع التشفيرالبسيط وفك التشفير ويتكون من 16 مرة لكل منهما. قوة خوارزمية Blowfish يعتمد على المفتاح الفرعي. في هذا البحث تم اقتراح وسيلة لتوليد مفتاح مستخلص من أجزاء من الصورة ويحدد حجم االمفتاح المستخدم مع blowfish الخوارزمية المستخدمة في تشفير النص.

1. Introduction

The algorithms used in computer systems are complex mathematical formulas that dictate the rules of how the plaintext will be turned into ciphertext. A key is a string of random bits that will be used by the algorithm to add to the randomness of the encryption process. The entities to be able to communicate via encryption, they must use the same algorithm, many times, and the same key. In some encryption technologies, the receiver and the sender use the same key, and in other encryption technologies, they must use different but related keys for encryption and decryption purposes [1].

2. Blowfish Algorithm

Blowfish, a symmetric block cipher and a Feistel network which follows simple Enciphering and Deciphering functions of 16 times each. The strength of the Blowfish algorithm relies on its sub-key generation and its basic confusion and diffusion based design.[2] Blowfish cipher uses 18 each of 32-bit Permutation arrays precisely known as P-Boxes and 4 Substitution boxes referred as S-Box each of 32 bit size and having 256 entries each. It uses a Feaster cipher which is a general method of transforming a function into another function by using the concept of permutation, diffusion, confusion [3].

The working of blowfish cipher can be illustrated as follows, It splits the 64 bit block into two equal blocks having 32 bit size each, left block is XORed with first Sub array P1 and thus obtained result is fed in to a function called F-function. Inside the F-function substitution operations are carried out which in turn converts 32 bit blocks in to another 32 bit blocks. Thus resulted 32bit entries are XORed with the right half and the result obtained is swapped as the left half for the next round. The Fiestal Structure of Blowfish Algorithm with 16 rounds of encryption is shown in the following Figs.1, 2, and 3.

3. Related work of key generator

A key generator is used in many cryptographicprotocols to generate a sequence with many pseudo-random characteristics. This sequence is used as an encryption key at one end of communication, and as a decryption key at the other.

The initial value of the LFSR is called the seed, and because the operation of the register isdeterministic, the stream of values produced by the register is

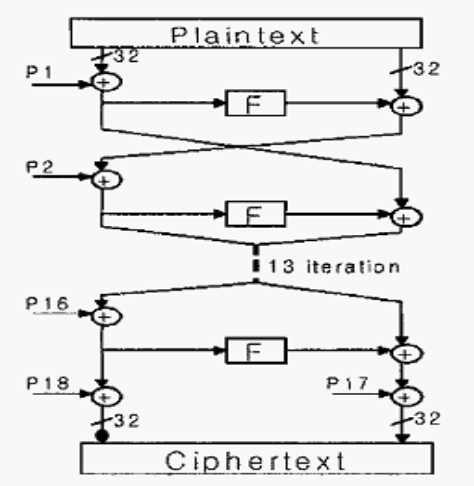

Figure (1) blowfish algorithm.

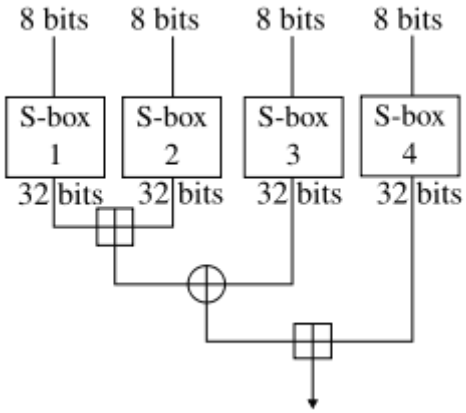

Figure (2) s-boxes to blowfish.

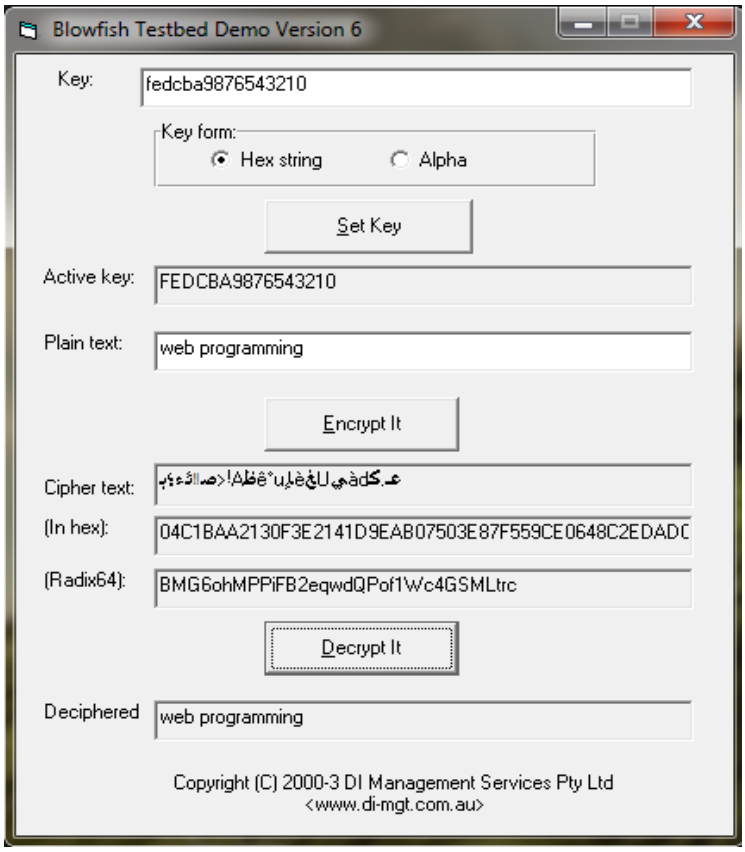

Figure (3) implementation of blowfish.

completely determined by its current(or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle [3,4].

Refer to a technique, its objective is the blending between the two encryption methods. Data Encryption Standard (DES) and Diffie Hellman to make DES more safe and secure. That by propose two options first one include injection the encryption DES after the seventh round with Diffie-Hellman just as key distribution algorithm then the results of the last back to the eighth round to complete the encryption process of DES. The second include injection the encryption DES after the eighth round with Diffie-Hellman just as key distribution algorithm to generate key the results of the eighth round will be encrypted using stream cipher then back to the ninth round to complete the encryption process of DES [5].

This tool generates a WPA encryption key that can be used to secure your Wireless network. Generate the WPA Encryption key, copy it and paste it into your wireless router's configuration panel. Restart your DSL modem/router.

WPA is designed for use with an 802.1X authentication server, which distributes different keys to each user. However, it can also be used in a less secure "pre-shared key" (PSK) mode, where every user is given the same passphrase. The Wi-Fi Alliance calls the pre-shared key version WPA-Personal or WPA2-Personal and the 802.1X authentication version WPA-Enterprise or WPA2-Enterprise[6].

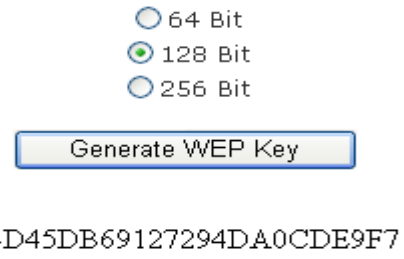

Fig.(4) web key generator 64,128,or 256 bit

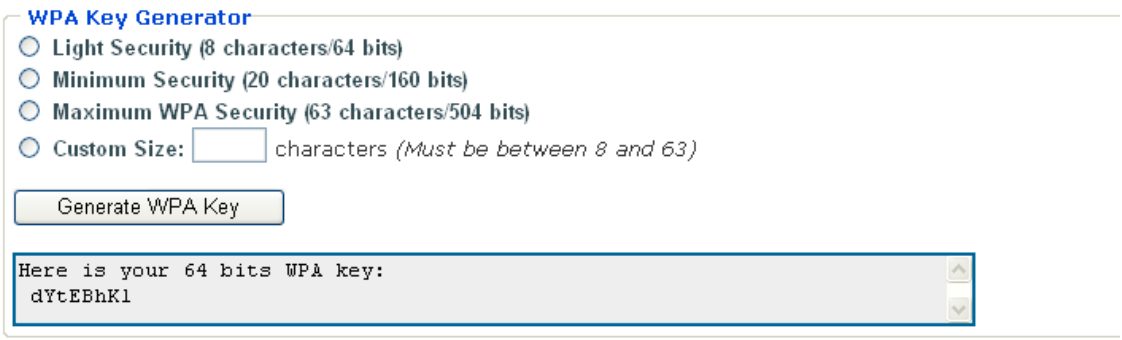

Fig. (5). Web key generator between 8-63 characters.

4. The Design of the Proposal

The proposed system suggests technique to derive the encryption key of any image are set by the user and determines the location of the points drawn from the key and depends on the colors red and blue and taking x or between the red and blue and a series of numbers is the key and determines its length according to Blowfish algorithm between 32-448 bit size.

Algorithm of proposal

Step 1: Load picture
Step 2: read picture by pixel and RGB
Step 3: get the key 32-448 bit size
Step 4: convert key to ASCII or Hex
Step5: use key to Blowfish Algorithm End

5. The Implementation of the Proposal System

The implementation of the proposal is using VB6 language. The application consists of several interfaces start to upload a photo as the user's choice and read the points and pull the two colors red, blue and the work of XOR. Then determines the length of the key according to the method used between 32-448 bit, (Figs. 6-10) to explain the proposal.

6. Conclusion

By studying the Blowfish algorithms and analysis its work, this research presents some modification on it. By implementing the proposed modified key of Blowfish there is some point concluded, these are:

The encryption of Blowfish has something danger, that it is an algorithm depend on symmetric key, so if the key is discovered that will destroy the Blowfish security. From previous point, the research proposes key generation method aim to reduce the danger of symmetric keys by

taking short key and from it the overall key will be generated.

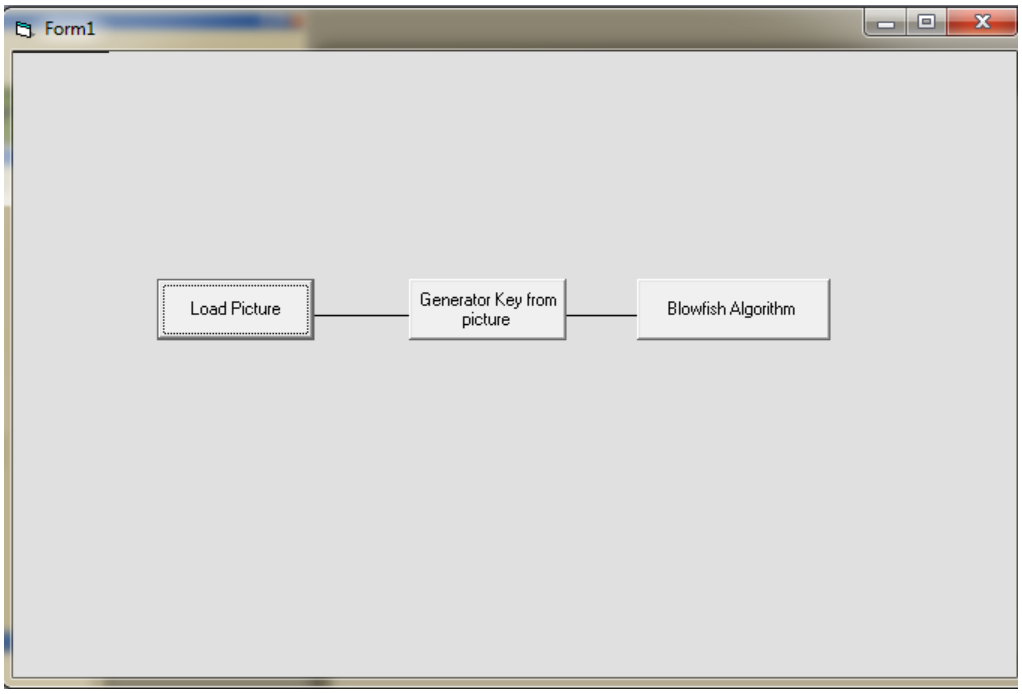

Figure (6) main proposal system.

In figure(7) The main application interface.

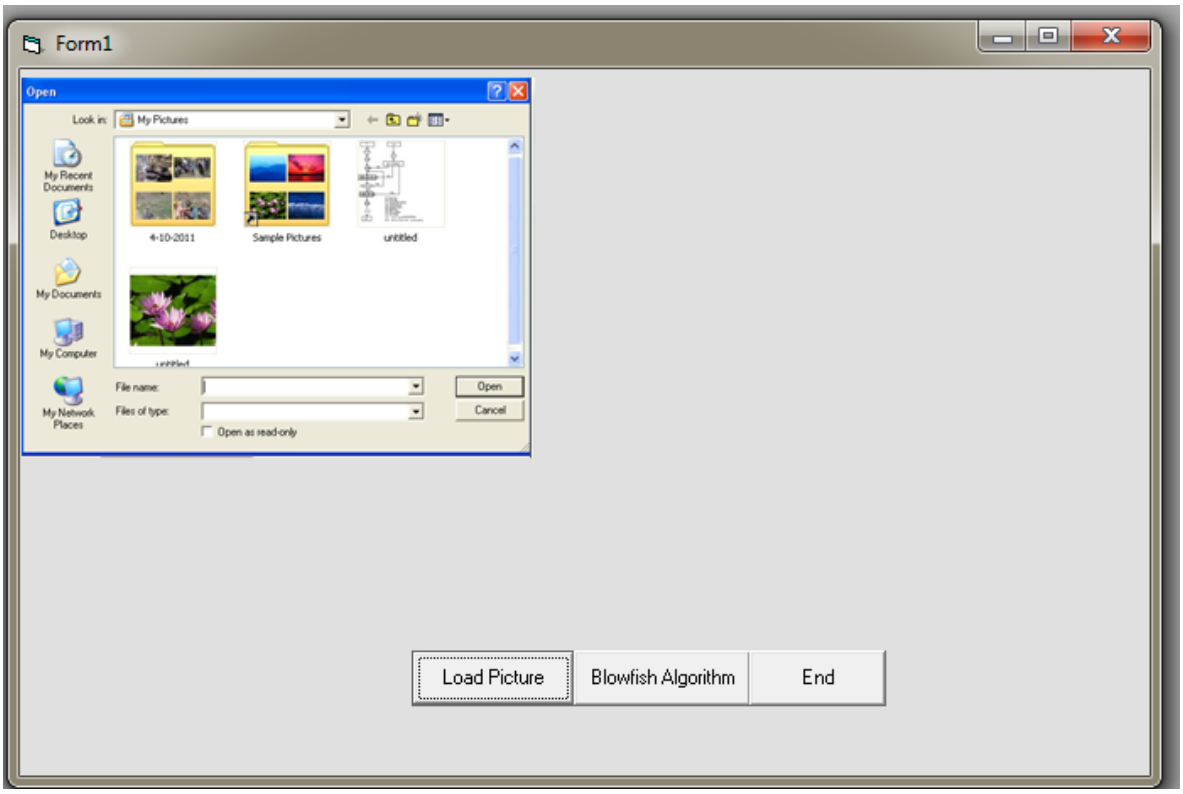

Fig.(7) main implementation load image

In figure (8) the second interface choose Key size

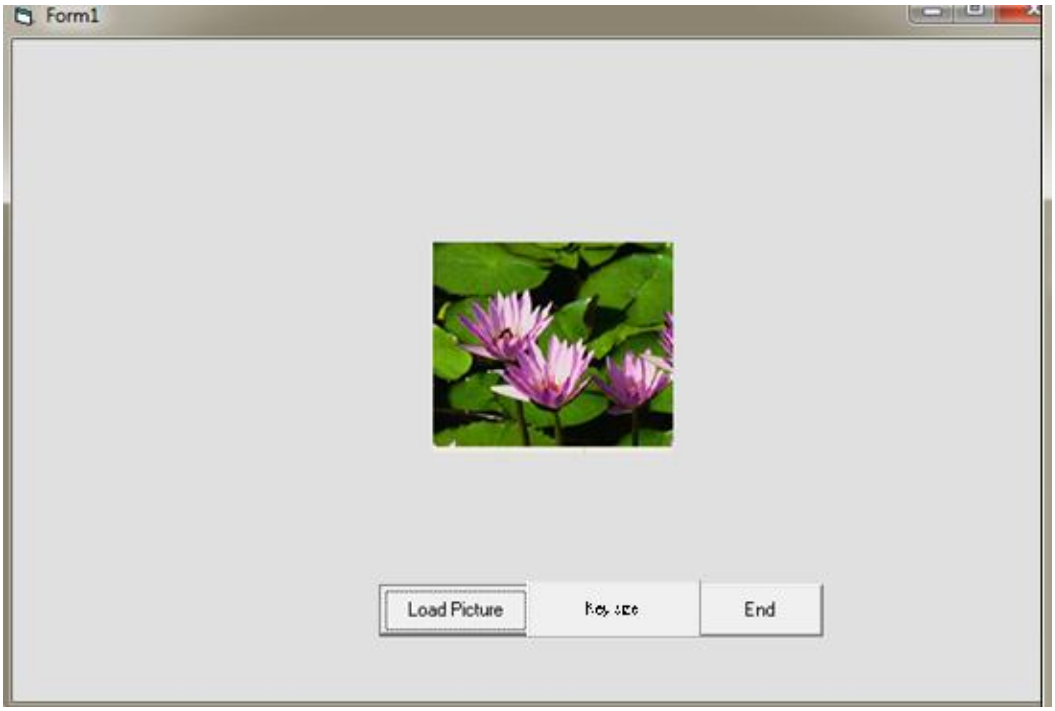

Fig. (8) Choose size of key.

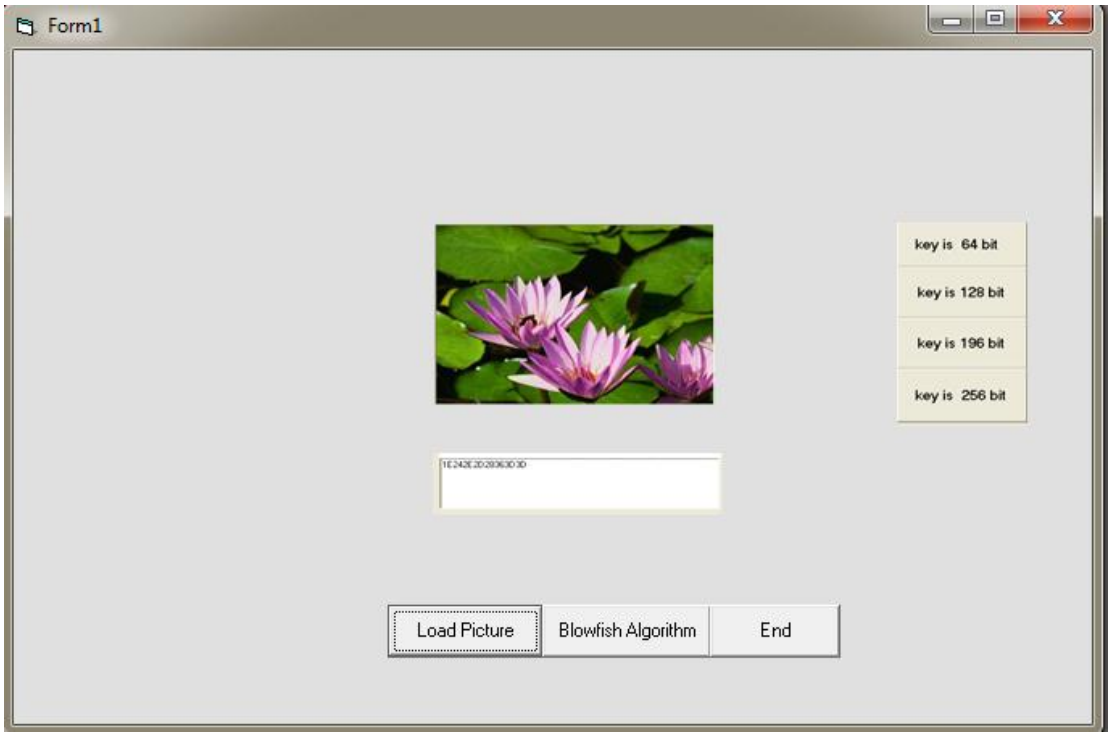

Fig. (9) Generator key.

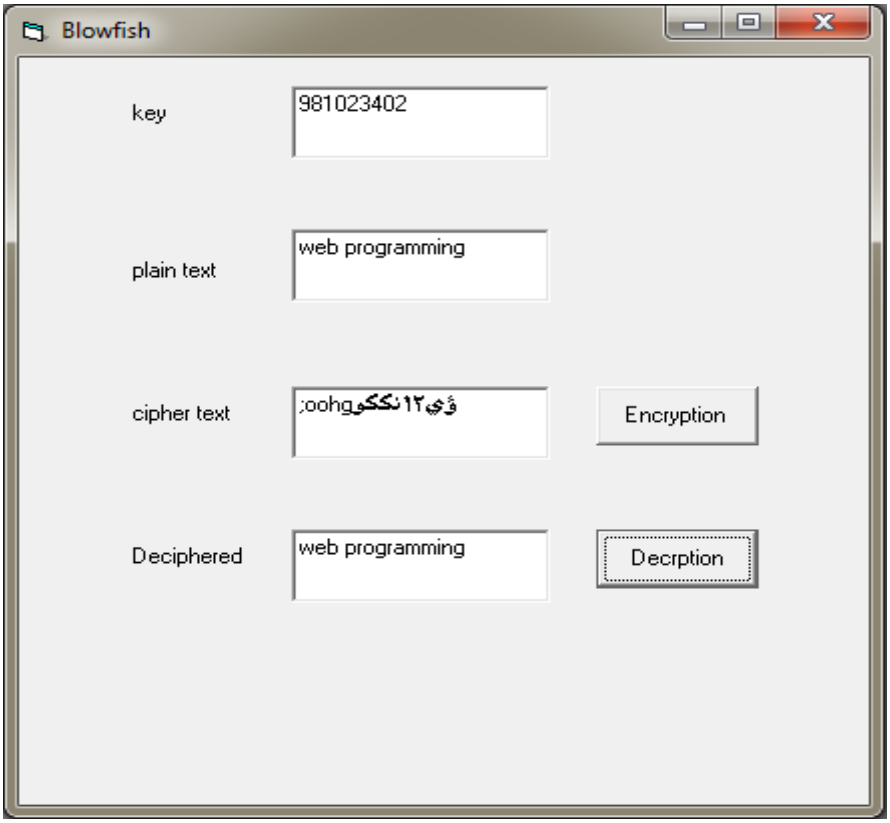

Figure (6) Blowfish proposal system.

References

1. Blowfish, http://en.wikipedia.org/wiki/Blowfish_(cipher)
2. "Type-3 Feistel Network of The 128-bits Block Size Improved Blowfish Cryptographic Encryption", Ashwaq T. Hashim Received on: 28/5/2008 Accepted on: 6/11/2008
3. Adam Young. "Mitigating insider threats to RSA key generation". Crypto Bytes, 7(1):1–15, 2004.
4. Encryption & decryption,

   http://www.encryptionanddecryption.com/encryption/
5. "Modification to Improve the Mobile-Commerce Security" A Dissertation Submitted to the department of computer science of university of technology in partial fulfillment of the requirement for degree of Doctor of philosophy in computer science by Soukaena Hassan Hashem, 2002 (77-90).
6. R.Satheesh Kumar, E.Pradeep, K.Naveen and R.Gunasekaran "**A Novel** Approach for Enciphering Data of Smaller Bytes" International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010.
7. Shatha Habeeb " *Proposal to Complex DES Security Using Diffie Hellman Injection* **",(**1216-1226) Engineering & Technology Journal Vol. 29, No. 6, 2011.