Proposal to Generate a Various Key from Image for Various Encryption Methods

Shatha Habeeb
University of Technology, Computer Sciences Department/Baghdad
Eman Shakeer
University of Technology, Computer Sciences Department/Baghdad
Email:uot_magaz@yahoo.com

Received on: 16/6/2011& Accepted on: 15/8/2012

ABSTRACT

There are three basic encryption methods: hashing, symmetric cryptography, and asymmetric cryptography. Each of these encryption methods have their own uses, advantages, and disadvantages. All three of these encryption methods use cryptography, or the science of scrambling data . Although there can be several pieces to an encryption process, the two main pieces are the algorithms and the keys. As stated earlier, 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.

This paper proposed a method which generates the key that draw from parts of the image. The size of the key is used with the suggested algorithm to encryption of the text. This method could be applied to Symmetric cryptography or Asymmetric cryptography.

Keywords: encryption keys, symmetric keys and asymmetric keys

مقترح لتوليد مفتاح ذات احجام مختلفة من الصورة لطرق تشفير مختلفة

الخلاصة

طرق التشفير الأساسية ثلاثة وهي : التجزئة والتشفير المتناظر والتشفير غير المتناظر. كل من هذه الطرق لها استخدامات خاصة بها، ومزايا وعيوب. كل هذه الطرق استخدمت التشفير ، أو علم تدفق البيانات. على الرغم من أن يمكن أن يكون هناك عدة أجزاء لعملية التشفير، والاجزاء الرئيسية هي خوارزميات ومفاتيح. وكما ذكر آنفا، الخوارزميات المستخدمة في أنظمة الكمبيوتر والمعادلات الرياضية المعقدة التي تملي قواعد الكيفية التي سيتم بها تشغيل مشفر في النص المشفر. مفتاح هو سلسلة من البتات العشوائية التي سيتم استخدامها من قبل الخوارزمية.

في هذا البحث تم اقتراح وسيلة لتوليد مفتاح مستخلص من أجزاء من الصورة ويحدد حجم االمفتاح المستخدم مع الخوارزمية المستخدمة في طرق تشفير النص، طرق التشفير المتناظر أو التشفير الغير متناظرة.

https://doi.org/10.30684/etj.31.1B.12
2412-0758/University of Technology-Iraq, Baghdad, Iraq

INTRODUCTION

Although there can be several pieces to an encryption process, the two main pieces are the algorithms and the keys. As stated earlier, 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. For two entities to be able to communicate via encryption, they must use the same algorithm and, many times, 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. The following sections explain the differences between these two types of encryption methods.

Cryptography is used to change readable text, called plaintext, into an unreadable secret format, called cipher text, using a process called encryption. Encrypting data provides additional benefits besides protecting the confidentiality of data. Other benefits include ensuring that messages have not been altered during transit and verifying the identity of the message sender. All these benefits can be realized by using basic encryption methods.

The first encryption method, called hashing, creates a unique fixed length signature of a group of data. Hashes are created with an algorithm, or hash function, and are used to compare sets of data. Since a hash is unique to a specific message, any changes to that message would result in a different hash, thereby alerting a user to potential tampering.

SYMMETRIC & ASYMMETRIC CRYPTOGRAPHY

Symmetric Cryptography In a cryptosystem that uses symmetric cryptography, the sender and receiver use two instances of the same key for encryption and decryption. Symmetric keys are also called secret keys, because this type of encryption relies on each user to keep the key a secret and properly protected. If an intruder were to get this key, they could decrypt any intercepted message encrypted with it .Common symmetric encryption algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and Blowfish.

Each pair of users who want to exchange data using symmetric key encryption must have two instances of the same key. This means that if Dan and Iqqi want to communicate, both need to obtain a copy of the same key. If Dan also wants to communicate using symmetric encryption with Norm and Dave, he needs to have three separate keys,Asymmetric or public key, cryptography is the last encryption method. This type of cryptography uses two keys, a private key and a public key, to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography in that a single key does not need to be securely managed among multiple users. In asymmetric cryptography, a public key is freely available to everyone while the private key remains with receiver of ciphertext to decrypt messages. Algorithms that use public key cryptography

include RSA and Diffie-Hellman. Bob encrypts data with his private key, the receiver must have a copy of Bob's public key to decrypt it. The receiver can decrypt Bob's message and decide to reply to Bob in an encrypted form. All she needs to do is encrypt her reply with Bob's public key, and then Bob can decrypt the message with his private key. It is not possible to encrypt and decrypt using the same key when using an asymmetric key encryption technology because, although mathematically related, the two keys are not the same key, as they are in symmetric cryptography. Bob can encrypt data with his private key, and the receiver can then decrypt it with Bob's public key. By decrypting the message with Bob's public key, the receiver can be sure the message really came from Bob. A message can be decrypted with a public key only if the message was encrypted with the corresponding private key [1, 2].

RELATED WORK

A key generator is used in many cryptographic protocols 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.

Examples of key generators include linear feedback shift registers (LFSR) and the Solitaire (or Pontifex) cipher. A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state.

The only linear function of single bits is xor, thus it is a shift register whose input bit is driven by the exclusive-or (xor) of some bits of the overall shift register value.

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

Refer to a technique it is objective is the blending between the two encryption methods 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 [4].

Create a WPA Key .This tool generate a WPA encryption key that you can use 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 [5, 6].

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 xor between the red and blue and a series of numbers is the key and determines its length according to the method used in the encryption in addition to being symmetrical or non-Symmetrical¯ In this research have been proposed 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 xor between the red and blue and a series of numbers is the key and determines its length according to the method used in the encryption in addition to being symmetrical or Asymmetrical**.**

THE IMPLEMENTATION OF THE PROPOSAL SYSTEM

The implementation of the proposal done by 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 and blue and the work of XOR them and determines the length of the key According to the method used and the user chooses the method of encryption is symmetric or asymmetric, where the asymmetric with either DES or AES and the length of the key 64,128,196 or 256-bit, with either asymmetric DES Diffe-Helmn determines the prime number**.**
In Figure (3) the main application interfaces Walt bearing the image of a particular site.In Figure (4) the second interface we choose symmetric or asymmetric
In figure (5) symmetric determines the length of the key with 64,128,196, or 256-bit with Hexadecimal. In Figure (6) determines the length of the key with 64,128,196, or 256-bit with ASCII. In Figure (7) choose Asymmetric Encryption with Hexadecimal and choose RSA or Diffie Helman and the generation of prime Number .In Figure (8) choose Asymmetric Encryption with ASCII and choose RSA or Diffie Helman and the generation of prime Number .

CONCLUSIONS

In all encryption algorithms symmetric or asymmetric still the key length and strongest of it the basic pointer for strongest encryption algorithm.

1. Our modest system could extract various keys with various length for various algorithms, that make the proposed system very flexible to deal with most of encryption methods.
2. Using the image as a pool for key extracting with our proposed methods of mixing R with B give the key much more randomness couldn’t be guessed by attackers.
3. To deal with most famous encryption method we provide the keys in both ASCII and Hexadecimal.

REFERENCES

[1].Adam Young. "Mitigating insider threats to RSA key generation". Cryp-toBytes, 7(1):1–15, 2004.
[2].http://www.encryptionanddecryption.com/encryption/

[3]. Venkateswaran Dr. V. Sundaram, R. Research Scholar- Ph.D Director-Computer Applications, Karpagam Academy of Higher Education Karpagam College of Engineering , Karpagam University, Affiliated to Anna University Coimbatore, Tamilnadu, India. Coimbatore, Tamilnadu, India " Information Security: Text Encryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 3 – No.7, June 2010

[4].Shatha Habeeb " *Proposal to Complex DES Security Using Diffie Hellman Injection* ", 2011 .

[5]. http://www.yellowpipe.com/yis/tools/WPA_key/generator.php

[6].P.Karthigaikumar Asst.Professor (SG) Department of Electronics and Communication, Karunya University,Coimbatore , Soumiya Rasheed M.Tech Department of Electronics and Communication Karunya University,Coimbatore "Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011 166

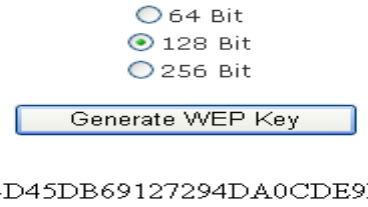

Figure (1) web key generator 64, 128, or 256 bit

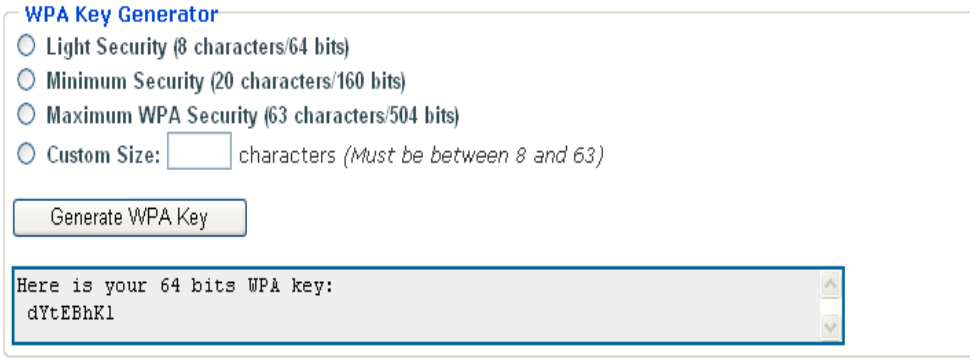

Figure (2) web key generator between 8-63 characters

Description of the Proposal algorithm

Input : select and read image , generator key from image
Output : key to using to any encryption methods
Process :
Step 1 : Load image.
Step 2: read image by pixel and RGB
Step 3: select the Encryption method and length of key
Step 4: get the key from R xor B

Step 5: convert key to ASCII or Hex
End

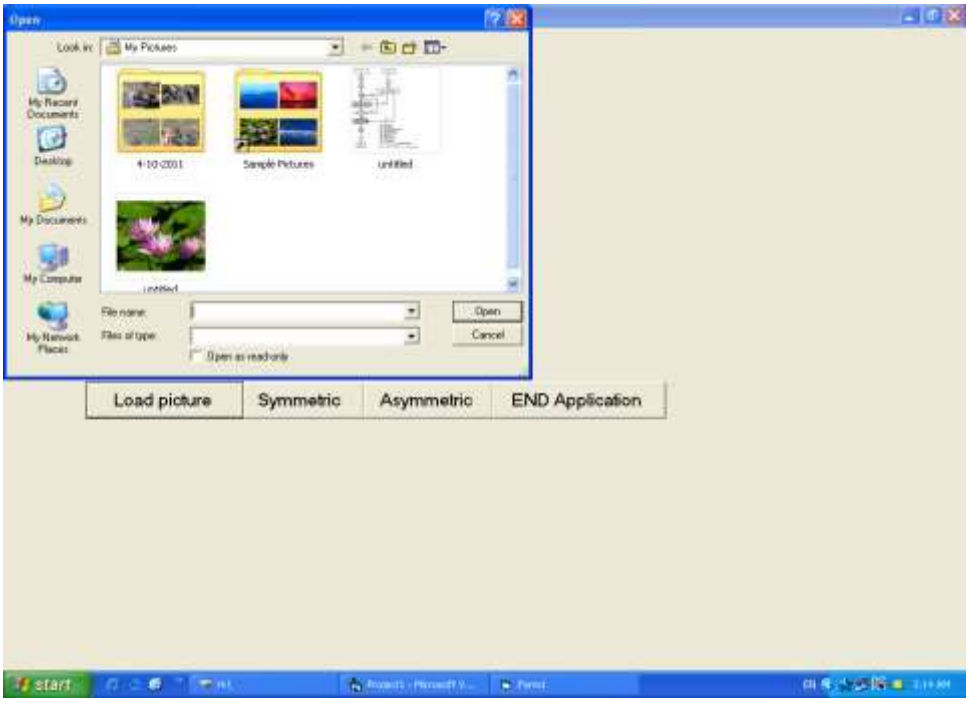

Figure (3) main implementation.

Figure (4) choose a symmetric or asymmetric.

Figure (5) symmetric Encryption with Hexadecimal.

Figure (6) symmetric Encryption with ASCII.

Figure (7) Asymmetric Encryption with Hexadecimal.

Figure (8) Asymmetric Encryption with ASCII.