Iraqi Journal of Computers, Communications, Control and Systems Engineering
Journal homepage: https://ijccce.uotechnology.edu.iq

Improvement of the Secret key Exchange in Symmetric Cryptography

Amer Kais Obaid Aljumaili

Control and Systems Engineering College, University of Technology, Baghdad, Iraq
Amer.k.obaid@uotechnology.edi.iq

DOI: https://doi.org/10.33103/uot.ijccce.25.1.8

HIGHLIGHTS

- The exchanging of the secret key using symmetric cryptographic.
- Exchange secret keys over insecure communication channel based on hybridizing the steganography using LSB

ARTICLE HISTORY

Received:11/January/2011

Revised: 20/March/2011

Accepted: 15/August/2011

Available online: 30/April/2025

Keywords:
Web security, Key Exchange, Cryptography, Confidentiality, Hiding Information, Steganography.

ABSTRACT

The important of reducing a chance of the information being detected during the transmission is Being an issue now days. Some solution to be discussed is how to passing information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. The exchanging of the secret key that used in symmetric cryptographic represents a major and the most sensitive part of symmetric cryptographic systems. In different studies, Cryptanalysts usually attack symmetric key cryptosystems through their key management. In this paper, we present a new algorithm to exchange secret keys over insecure communication channel. This algorithm is based on hybridizing the steganography based on LSB (Least Significant Bit) stenography with cryptography using XOR function for exchanging the secret keys. It provides security and reasonable computational cost. Furthermore, it restricts most of the current attacking mechanisms.

I. INTRODUCTION

The Internet provides an excellent vehicle for increasing transaction efficiencies and extending the scope of communication and business. The Internet is a public, insecure network. Basically all information sent to the Internet is public. One essential aspect for secure communications is that of cryptography [1].

Cryptography provides the mechanisms necessary to provide accountability, accuracy and confidentiality in inherently public communication mediums such as Internet. Today, cryptographic processing is primarily reserved for electronic commerce transactions and secure e-mail, will subject more of all communication to cryptographic processing [2]. The rest of the paper includes the following: section II presents the overview of cryptography. Section III introduces steganography, and hiding information which is based on Least Significant Bit Insertion. Section IV and V obtains the proposed algorithm and implementation, while section VI concludes the paper.

II. CRYPTOGHRAPHY

Cryptography is the art of achieving security by encoding messages to make them non-readable. There are two basic types of cryptography: Symmetric Key. Symmetric Key cryptography, also known as secret key cryptography, which requires the sender and receiver of a message to share the use of a single, common key for encryption and decryption. Asymmetric Key cryptography, also known as public key cryptography, which employs two keys: a public key to encrypt messages and a private key to decrypt them [1].

A. Symmetric Cryptography

In Symmetric cryptography (secret key cryptography), a single hey is used for both encryption and decryption. As shown in *Fig. 1*, the sender uses the key to encrypt plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single hey is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this algorithm is the distribution of the key [l][3].

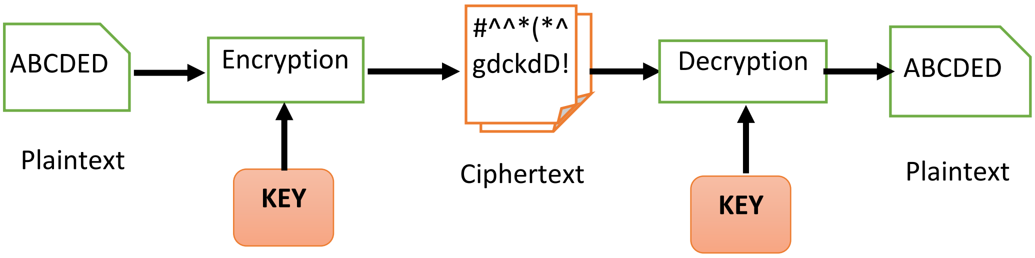

FIG. 1. PROCESSING OF SYMMETRIC CRYPTOGRAPHY.

B. Asymmetric Key Cryptography

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission, as shown in *Fig. 2*. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised [1]. On the other hand, the public key cryptography is poorly suited for encrypting large messages [4].

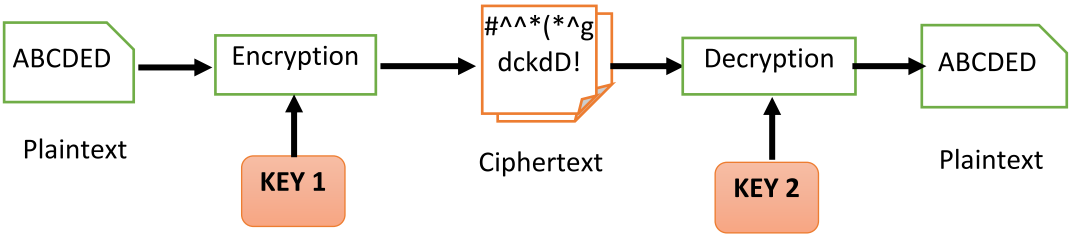

FIG. 2. PROCESSING OF ASYMMETRIC CRYPTOGRAPHY.

The main problem with symmetric ccryptography is distribution of private key. To securely share a private key, communicating parities would first have to be holding a shared a private key, and need to have a secure channel to transmit the key through it [5]. If this secure channel is compromised the they in transmission may be vulnerable to interception by attackers because the Inter net is unsecure transmission media.The important of reducing a chance of the secret key being detected during the transmission, some solution discussed is to manage passing the secret key. There are two solutions to manage the secret key passing via unsecure media; first, by using public-key cryptography [6]. For all benefits of the first solution, still the public-key cryptography not providing a comprehensive solution to the key management problem a disadvantage of using public-key cryptography for encryption is the speed.

Another solution is by. sending symmetric key cryptography in unknown in order to repel attention of the potential attacker. We can use Steganography to hide this key in a digital image. We focus on the Least Significant Bit (LSB) technique to hide secret key in a digital image [7].

C. Steganography

Steganography is the process of hiding one file inside another such that others can neither identify the meaning of the embedded object, nor even recognize its existence. Current trends favor using digital image files as the cover file to hide another digital file that contains the secret message or information. One of the most common methods of implementation is Least Significant Bit Insertion, in which the least significantt bit of Every byte is altered to form the bit-string representing the embedded tile. Altering the LSB Will only cause minor changes in color, and thus is usually not noticeable to the human eye. While this technique works well for 24-bit color image files, Steganography has not successful when using an 8-bit color image file due to the limitations in color variations and using color map [8].

D. Least Significant Bit Insertion

One of the most common techniques used in stenography today is called the least significant (LSB) insertion. This method is exactly what it sounds like; the least significant bits of the cover-image are alerted so that they form the embedded information. The advantages of LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover -image and many techniques use these methods. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small [8].

III. RELATED WORK

Many Published work on symmetric cryptographic has focused in new algorithms on speed of the implementation of ciphering algorithms as well as increase the complexity of cryptanalysis by the attackers. Ayushi [1]: The aim of this paper was to design and implement a new algorithm to achieve few goals like Confidentiality, Data integrity, Authentication of the send the data, taking into account the cost-effective. But it did not focus on the process of secret key exchange over insecure channels such as Internet. Jerome B. John McDonald Todd A. [2]: proposed new instruction that speed the common operations of symmetric ciphers. instruction set support is added for substitutions, permutations, rotates, and modular multiplication. Also exploring the implications of a design where the primary purpose of processor is cryptographic processing. Cryptographic processors would have to deliver orders magnitude more performance to meet the bandwidth demands of secure servers and virtual private network (VPN) routers. In this paper we focus on problem of exchange the secret key over insecure channels.

IV. PROPOSED ALGORITHIM

We propose a web security mechanism that supports the confidentiality and security for exchanging secret key along the communication path between the sender and the receiver. Such a mechanism can be done by an algorithm between them. This algorithm based on hiding information using the stenography. We use an image file as a carrier to hide secret encrypted key used in symmetric key cryptography. Therefore, the carrier will be known as cover-image, while the stego-object known as stego-intake. The implementation of system will only focus on Least Significant Bit (LSB) as one of the stenography techniques as mentioned in previous section 3. The proposed algorithm is composed by a Hiding XOR Encryption (HidXEncry) at sender side and a Hiding XOR Decryption (HidXDecry) at recipient side:

A. Hiding XOR Encreption Algorithim

In the following steps for implelemntation of Hiding XOR Encryption (HidXEncry) at sender side

Alg: *HidXEncryy.*
Input: *Plaintext, Cover Image.*
Output: *Stenography Image*
Process:

Step 1: generating Secret Ke y randomly ***SK****.*

Step 2: Encrypting the information ***M*** *with secret key to generate Ciphertext* ***C=M(SK)****. Step 3: Convert Secret Key to ASCII Code* ***SK******

Step 4: Converting SK ASCII into 8 bit binary.*

Step 5: Generating second Random Key [8 b it binary value] ***RK****.*

Step 6: Encrypting ***SK****’ with XOR function with* ***RK*** *to result (**SK * $\oplus$ RK**).*

Step 7: Convert image to ASCII Code, then into 8-bit binary.

Step 8: Set LSB=0, and bit replacement with ***RK****.*

END

B. Hiding XOR Decryption Algorithm

In the following steps for implelemntation of Hiding XOR Decryption (HidXDecry) at recipient side

Alg: *HidXDecry.*
Input:*, Stenography Image.*
Output: *Plaintext*
Process:

Step1: Execrating ***RK****.*

*Step 2: Decrypting (**SK*$\oplus$RK**) using XOR function with* ***RK*** *to result* ***SK*.***

Step 3: Decrypting ciphertext symmetric cryptography ***SK**** *to obtain the plaintext.*

END

V. IMPLEMENTATION

When sender wants to send secret information to recipient must be sending in ciphertext using symmetric cryptography to keep confidential of this information. The sending of the symmetric key cryptography is done by encrypting it with XOR Function, and then hiding in digital image by using stenography as obtain in 5.1. The recipient receives ciphertext and steno-image, to enciphering secret information as shown in 5.2. *Fig. 3* shows the flowchart of the new approach to Secret key Exchange.

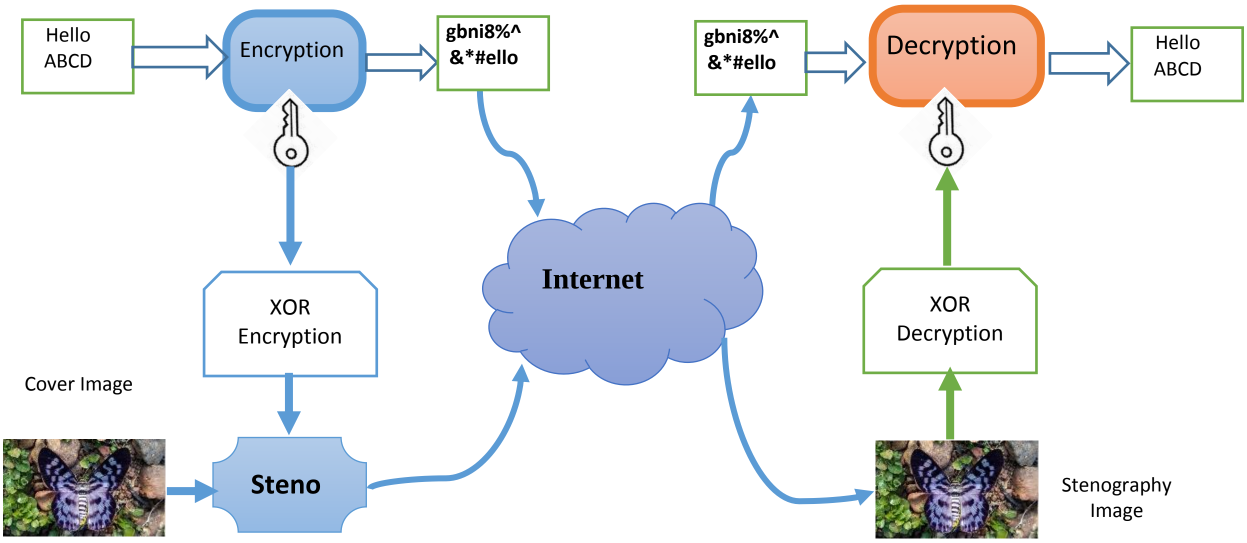

FIG. 3. THE GENERAL FLOWCHART OF THE NEW ALGORITHM TO SECRET KEY EXCHANGE.

A. Sender Side

When the sender wants to exchange secret information with others, the following operations must be done:

1. It is very important that the Secret key is generated randomly SK.

2. Encrypting the secret information with secret key cryptography to generate Ciphertext **C=M(SK).**

3. Convert Secret Key to ASCII Code **SK***.

4. Converting **SK*** ASCII into 8-bits binary.

Example: the secret key **SK**: **A2%fhbv45&,** then the ASCII Code of this key is (**SK***), as shown in the Table I.

TABLE I. ASCII CODE OF THE **SK**

Char (*SK)*	A	2	%	f	h	b	v	4	5	&
ASCII (*SK* *)	65	50	37	102	104	98	118	52	53	38
Binary (*SK* *)	**01000001**	**00110010**	**00100101**	**01100110**	**01101000**	**01100010**	**01110110**	**00110100**	**00110101**	**00100110**

5. Generating second Random Key [8 bits binary value] : **RK**.

6. Encrypting **SK*** with XOR function with **RK** to result (**SK* ⊕ RK**) as shown in the Table II and *Fig. 4*.

TABLE II. ENCRYPTING SK* WITH XOR FUNCTION WITH RK

Binary	01000001	00110010	00100101	01100110	01101000	01100010	01110110	00110100	00110101	00100110
XOR with (RK)	10011010	10011010	10011010	10011010	10011010	10011010	10011010	10011010	10011010	10011010
(SK* ⊕RK)	11011011	10101000	10111111	11111100	11110010	11111000	11101100	10101110	10101111	10111100

7. Loading digital image as carrier and convert image to ASCII Code, then into 8-bit binary, then Set LSB =0, and bit replacement with M.

8. Sending the ciphertext, encrypted secret key (***SK** * **⊕RK***), and Steno-image to the recipient.

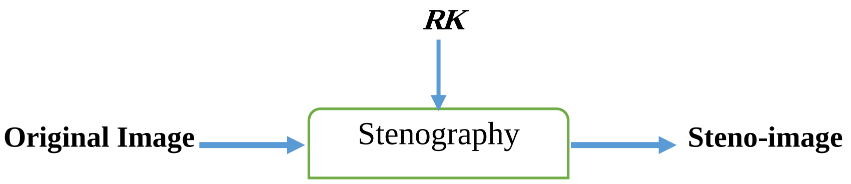

FIG. 4. STENOGRAPHY PROCESSING FOR ORIGINAL IMAGE.

B. Recipient Side

After the recipient receives the ciphertext, encrypted secret key (**SK* ⊕ RK**), and Steno-image, the following operations must be done:

1. Checking the format of Steno-image extracting **RK**, the cryptography.

Steno-image → **Original Image** + ***RK***

2. Decrypting (**SK* ⊕ RK**) using XOR function with **RK** to result **SK*** as shown in the Table III.

TABLE III. DECRYPTING (SK* ⊕ RK) WITH XOR FUNCTION WITH RK

(*SK** *⊕RK*)	11011011	10101000	10111111	11111100	11110010	11111000	11101100	10101110	10101111	10111100
XOR with (RK)	10011010	10011010	10011010	10011010	10011010	10011010	10011010	10011010	10011010	10011010
*SK**	01000001	00110010	001001001	01100110	01101000	01100010	01110110	00110100	00110101	00100110

3. Decrypting ciphertext symmetric cryptography **SK*** to obtain the plaintext.

VI. CONCLUSION

Confidentiality considerations are very important and sensitive part of the infrastructure security in modern computer networks. In this paper, the proposed algorithm is new method to exchange the symmetric key cryptography in secure manner. The user can easily encrypt information and send them through a public channel or insecure media. The proposed method can enhance confidentiality of sharing information in internet, and share secret key and provide a privately communication between the recipients.

REFERENCES

[1] A, Ayushi “A Symmetric Key Cryptographic Algorithm” 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15.

[2] J. Burke, J McDonald, T Austin. "Architectural support for fast symmetric-key cryptography." In Proceedings of the ninth international conference on Architectural support for programming languages and operating systems, pp. 178-189. 2000.

[3] B.A. Carter, A Kassin, T Magoc. "Symmetric Cryptosystems and Symmetric Key Management." CiteSeerX 10, no. 1.135 2007.

[4] D. Kuhn, V Hu, W Polk, S Chang. Introduction to public key technology and the federal PKI infrastructure. No. NIST Special Publication (SP) 800-32 (Withdrawn). Gaithersburg, MD: National Institute of Standards and Technology, 2001.

[5] B.,Schneier. Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.

[6] I., Curry. "An introduction to cryptography and digital signatures." Entrust Securing Digital Identities and Information (2001).

[7] MM, Amin, M, Salleh, S, Ibrahim, M, Katmin, and M. Z. I. Shamsuddin. "Information hiding using steganography." In 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings., pp. 21-25. IEEE, 2003.

[8] M. Juneja, PS Sandhu, E Walia. "Application of LSB based steganographic technique for 8-bit color images." World Academy of Science, Engineering and Technology 50 (2009): 423-425.