HOW TO OBTAIN HIGH SECURITY OVER THE E-COMMERCE SYSTEM

Vasin Suttichaya[1,2] and Pattarasinee Bhattarakosol[1,3]

[1]Department of Mathematics, Faculty of Science,
Chulalongkorn University, Bangkok, 10330, Thailand
[2]vasin.s@student.chula.ac.th, [3]pattarasinee.b@chula.ac.th

ABSTRACT

Today, E-commerce is a comfortable choice for trading. Many organizations use e-commerce as a main path for their business. The secret of information for communicating between participants are significantly important. Many methods of cryptography are applied for protecting the secret of information in the e-commerce system, such as 3DES, AES, and ECC. Many protocols for e-commerce systems are also created for serving this requirement. However, those methods are proved that they are computational secrecy, not perfect secrecy. One-Time Pad (OTP) is the only one method that is proved to be perfect secrecy. Unfortunately, OTP has never been implemented in the real application, except the applications that require more security, such as a code for releasing the nuclear missile, because OTP has a problem of the key for encrypting/decrypting the plaintext since it must be as long as the plaintext. From this factor, it leads to many problems for managing the applications that use OTP, such as the key management problem and the real random number generator problem. This paper proposed a method called KAEW, or Key-chaining Algorithm for Encrypting/decrypting Word Block, to encipher all types of the plaintext. The result of using this method serves the perfect secrecy of OTP.

Index Terms— One-Time Pad, Cryptography, Encryption, Decryption, Perfect Secrecy

1. INTRODUCTION

Electronic commerce or E-commerce was introduced in the early 1970, started by electronic money transfer process between organizations. In the beginning, e-commerce is used only in the large enterprise. According to fast development of the personal computer and the Internet, these factors advocate many organizations in using E-commerce as the main electronic data interchange. Today, E-commerce is used in many business transactions, such as online augmentation, online service, online trading, and so on.

The security of information over E-commerce environment is critically important. If an unauthorized person obtains access to the transferred information over the Internet, the organization can be corrupted. The major obstacle to E-commerce is concerned over insecure transactions because the Internet is the open system. The security of the information can be divided into three characteristics: confidentiality, integrity, and availability. Many methods are developed for serving these three characteristics, such that the digital-signature, hash functions, and cryptographic methods. In this paper, the only cryptographic is considered. Cryptography is a science of communication over the untrusted channels. The main point of the cryptographic method is to serving confidentiality of the information.

Cryptographic can be classified into 2 categories: the symmetric-key, and the asymmetric-key cryptography. In the symmetric key cryptography, or as known as the private key cryptography, a key to encrypt a plaintext and decrypt the cipher text is the same key. On the other hand, the asymmetric key technique, or can be called as the public key cryptography, uses a public key for encrypting a plaintext but it uses a private key to decrypt the cipher text. Both symmetric and asymmetric keys cryptographies have advantages and disadvantages. The symmetric key cryptography can calculate in a small amount of time. Nevertheless, this technique has the key distribution problem. Thus, the asymmetric key cryptography is implemented to solve the problem of key distribution but the calculation time is longer than the use of the symmetric key technique.

Currently, many cryptographic methods, both symmetric-keys and asymmetric-keys, are embedded in the E-commerce system, for instances 3DES, AES, RSA and so on. Unfortunately, these methods can serve only computational secrecy but not perfect secrecy. The only method that serves the perfect secrecy is One-Time Pad (OTP) [1], [2]. If the sender uses OTP for encrypting a message, no matter what computational power and time eavesdropper has, he or she could not extract the plaintext without the key. However, OTP is not use in the E-commerce system because OTP needs the real random generator for generating the key, and the key's length is as long as the plaintext. Moreover, since the key of OTP is very long, it causes key management problem.

This paper, the development of a new cryptographic method based on OTP method is proposed and integrated into the E-commerce system for serving the perfect secrecy. This paper is organized as follow. In section 2, the related works will conclude general cryptography algorithms that widely use in E-commerce system. In section 3, the One-Time Pad method is described in depth. In section 4, the KAEW is proposed. In section 5, the integration of the KAEW to E-commerce is described. In section 6, the advantages of KAEW are discussed. The last section is conclusion that will conclude overall of this paper.

2. RELATED WORK

It is a fact that the secret of the E-commerce's data is very vital; several cryptography methods are created for serving this requirement. Those methods, except OTP, do not serve the perfect secrecy. Furthermore, the computational rate is rapidly growth, which makes cryptanalyzers are able to break those methods in a short time, such as DES (Data Encryption Standard) [1], [3]. DES needs 56 bits key's length and 64 bits block size. According that the DES's key is very short, the power of the present computer can break DES without the key in a few hours. Thus, DES is now considered to be unsecured for many applications, including the E-commerce system. So many methods are developed to replace DES, such as 3DES and AES. For 3DES (Triple-DES) [1], [4], it uses DES 3 times for encrypting the information and needs 112 bits or 168 bits key's length. The 3DES's key is in the form of (K1, K2, K3) and each key contains 56 bits. In the case of 112 bits key, K1 is equivalence to K3. According to AES (Advanced Encryption Standard) [1], [5], [8], it allows using various key's lengths and block sizes. However, the new standard allows using the mix key's length between 128, 192, or 256 bits, including the blocking size.

One of public key cryptography methods that use in the E-commerce system is RSA [1], [6]. It can use in both encryption and digital signature and widely used in electronic commerce protocols. RSA is believed to be secured given significantly long keys. Encryption and decryption process can be performed by mathematical theory (Exponentiation and Modula). Generally, the key's length used in the Internet is 1,024 bits. So, RSA takes a long time comparing with the symmetric key encryption algorithm. Practically, RSA always uses with 3DES using RSA for key distribution and uses 3DES for encrypting the message.

Consider other public key methods, Diffie-Hellman and ECC (Elliptic Curve Cryptography) [1]. The concept of Diffie-Hellman is "the exponential is easier to calculate more than logarithm". Diffie-Hellman key exchange is a cryptographic protocol that allows two parties, that have no prior knowledge of each other, jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key encryption. This algorithm allows the sender and the receiver create a secret key for encrypting the message and eavesdropper cannot know the key that shares between them. The secret key can be calculated by its own private key and the partner public key. For ECC, its algorithm bases on Elliptic Curve Theory. This method can provide more security while uses the shorter key than RSA and other asymmetric key algorithms. So, it can calculate faster comparing with other asymmetric key algorithms. However, ECC is faster in decryption but it is slower when using in encryption when compare to RSA.

One acceptable method that was claimed to be the perfect cipher mechanism is the One-Time Pad that invented by Vernam [1], [2]; this method will be described as follow.

3. ONE-TIME PAD (OTP)

One-Time Pad, invented by Vernam, is a perfect cipher mechanism. Moreover, the concept of OTP is very easy to implement in both software and hardware. The OTP encryption and decryption methods are defined in (1) and (2) respectively.

$$c_i = p_i \oplus k_i, \quad 1 \le i \le n \tag{1}$$

$$p_i = c_i \oplus k_i, \quad 1 \le i \le n \tag{2}$$

where n is the number of plaintext's digits; $c_1, c_2, c_3, \ldots, c_n$ are the cipher text digits; $p_1, p_2, p_3, \ldots, p_n$ are the plain text digit; $k_1, k_2, k_3, \ldots, k_n$ are the key stream digits; and $\oplus$ is the exclusive-OR operation.

Before a sender and a receiver use the OTP, they must agree on a key which is in the form of a key stream randomly generated with the same length of the plaintext. By the time the sender encrypts the plaintext, the sender performs the XOR operation between a key and the plaintext. When the receiver decrypts the cipher text applied the key to the cipher text again. After that, the key will be eliminated.

The main concept of the OTP is that the security of any plaintext can be achieved whenever the key was completely generated by a truly random number, safety distributed, and used only once. Thus, illegal interception of a message is useless without the key [1], [2], [7].

3.1. Example of OTP

Let the encryption and decryption functions are defined as (3) and (4) respectively.

$$c_i = (p_i + k_i) \bmod 26, \quad 1 \le i \le n \tag{3}$$

$$c_i = (p_i - k_i) \bmod 26, \quad 1 \le i \le n \tag{4}$$

where n is the number of plaintext's character; $c_1, c_2, c_3, \ldots, c_n$ are the cipher text character

$p_1, p_2, p_3, \ldots, p_n$ are the plain text character; $k_1, k_2, k_3, \ldots, k_n$ are the key stream character.

Let the plaintext be defined as "secret"; it is encoded by Table 1 and encrypted using eq.3 with the key (19, 21, 7, 4, 11, 14). The output, cipher text, is "LZJVPH". Assume that the attacker uses Brute-force attack with some guess of possible keys, such as (9, 14, 5, 0, 11, 16) or (11, 6, 16, 21, 13, 23). Thus, the result of decrypting mechanism can be "clever" and "attack" respectively. So, the real plaintext is still blind from the attacker.

Table1. Encode Alphabet to Numeric Table

Alphabet	a	b	c	...	z
numeric	0	1	2	...	25

Let the plaintext be defined as "secret"; it is encoded by Table 1 and encrypted using eq.3 with the key (19, 21, 7, 4, 11, 14). The output, cipher text, is "LZJVPH". Assume that the attacker uses Brute-force attack with some guess of possible keys, such as (9, 14, 5, 0, 11, 16) or (11, 6, 16, 21, 13, 23). Thus, the result of decrypting mechanism can be "clever" and "attack" respectively. So, the real plaintext is still blind from the attacker.

Since the computing world has no real random number, but it uses the pseudorandom system to generate random number. Thus, the generated number will be random in a certain period of time and then the recycling starts. Thus, each key must be used only once for each message. Otherwise, with the cipher text, the cryptanalyst can recover the plaintext easily. Moreover, in order to obtain a perfect protection of a plaintext, the stream key of OTP must have length equal to the plaintext.

4. KEY CHAINING ALGORITHM FOR ENCRYPT/DECRYPT WORD BLOCK (KAEW)

Referring to the previous section, the disadvantage of OTP based on the OTP's key length. OTP needs a key's length long as the plaintext, which, in fact, is very long and not flexible to be transferred across the Internet or network. Moreover, OTP needs the real random generator for generating the key. According to those issues, OTP has never been used in the real applications, except for the applications that need high security. In this paper, the KAEW is implemented based on OTP by reducing the length of the OTP's key and reserves perfect secure of OTP by generating the key using real timing and always changing the seed value of the random number generator.

The KAEW has two keys for encrypting and decrypting plaintext: a main key, and sequenced keys. The process works by implementing OTP as the strongest algorithm for encrypting the first block of the information. The reason to use the OTP technique is that OTP is completely unbreakable symmetric cipher when the truly random key is used. The key for encryption in the OTP method is the main key of this algorithm. This main key is used for encrypting and decrypting the first block of the information. The main key comes from a truly random number, and the length of the key is the length of the block. Therefore, the random number is applied only to the first block of the segmented information. Thus, the length of the random number is based on the length of the segmented block, which is not long for the OTP mechanism. Then, the first block of the plaintext will be applied to the key generator function for generating a sequenced key for encrypting the next block of the plaintext, and so on. These subsections will be described in deep detail of sequenced key generator and encryption/decryption process of the KAEW respectively.

4.1. Sequenced Key Generator

The entire algorithm for generating the sequenced key is as follows:

Assume that a plaintext and a cipher text are in form of binary data. Seed values and the number of iteration are required in the sequenced key generator.

1) Import previous block of the plaintext and convert to a decimal value.
2) Combine the decimal value with other seed values.
3) Send the combined value and other seed values to the random function.
4) Iterate the random function until meets the number of iteration.
5) Convert the last random combined data to binary digits and exclusive-or the result with last random of other seed values.
6) Return the key and new seed values.

4.2. KAEW's Encryption Process

KAEW's encryption process is as follows:

1) Choose a main key and the seed values. Suppose that main key has length n digits.
2) Copy the first n bits of the plaintext to the safety register.
3) Encrypt the first n bits of the plaintext by OTP with a main key.
4) Apply the value in the safety register and the seed values to the sequenced key generator to obtain the sequenced key and new seed values for start calculating the next round. Suppose that the sequenced key has length m digits.
5) Copy backward m bits of the plaintext to the safety register.
6) Encrypt the backward m bits of the plaintext by OTP with the sequenced key.
7) Repeat steps 4-6 until the last bit of the plaintext is encrypted.

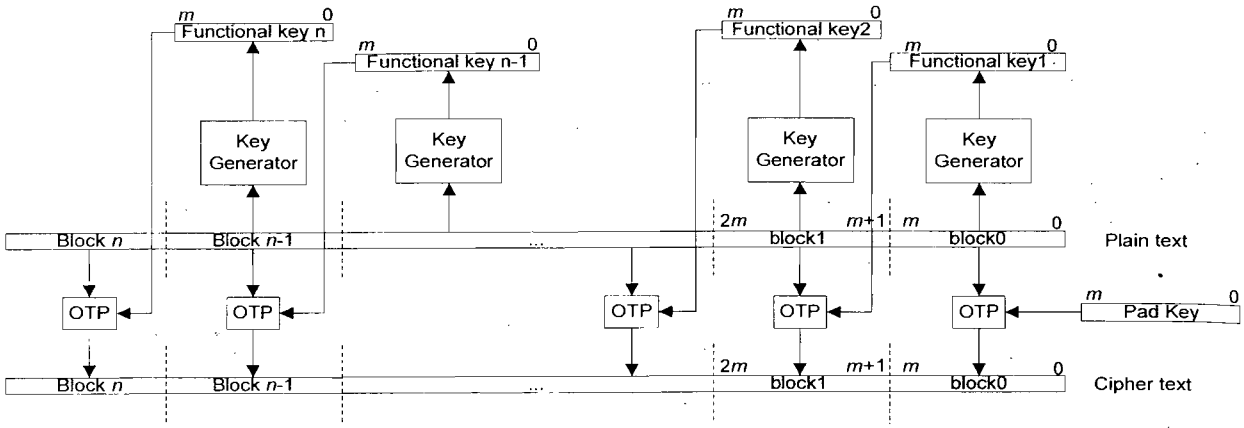

Figure 1. The overall of KAEW's encryption process

The overall process of KAEW encryption is shown in Figure 1.

4.3. KAEW's Decryption Process

In the decryption process, the reverse version of the encryption algorithm is described as follows:

1) Decrypt the first *n* bits of the cipher text by OTP with a main key to obtain the plaintext of the first block.
2) Copy the first *n* bits of the plaintext to the safety register.
3) Apply the value in the safety register to the sequenced key generator in order to obtain the sequenced key and new seed values for start calculating the next round. Suppose that the sequenced key has length m digits.
4) Decrypt the backward *m* bits of the plaintext by OTP with the sequenced key.
5) Copy backward *m* bits of the plaintext to the safety register.
6) Repeat steps 3-5 until the last bit of the cipher text is decrypted.

5. INTEGRATED KAEW TO THE E-COMMERCE SYSTEM

Consider the OSI model, the cryptographic process can be perform in Applications, Session, Transport, or Network Layers, each having its own advantages and disadvantage. The KAEW can be integrated to any layers of OSI because the KAEW is very flexible to be implemented. The recommend for the KAEW is the need of a session key as a main key because KAEW is implemented based on OTP. However, the KAEW needs to use the main key only once. Session keys must be chosen so that they are unpredictable by attackers. In the usual case, this means that they must be chosen randomly. Failure to choose proper session keys (or any keys) can be leaded to any cryptanalysis for cracking the cipher text. Although cryptanalyzers are able to guess the main key of the KAEW, they definitely face with many possibilities of seed values. Due to seed values for generating the sequenced key is changing from time to time, it is hard to guess what the initial seed values are.

6. DISCUSSION

Since the E-commerce's information is considerably vital to every business organizations, therefore, cryptosystem must play a significant role to protect the plaintext transferring over the Internet. Various methods have been proposed and implemented, such as DES, AES, RSA, ECC, and so on. Unfortunately, these methods, except OTP, are serve only computational secrecy. Different from other methods, the proposed method called the KAEW, a chain rule mechanism, is implemented by applying OTP. Moreover, it reduces the length of the key defined by the original OTP mechanism without reducing the secrecy of the transferring text. The major concept of the KAEW is the main key's length can change for fitting to any types of information. Moreover, the block size of the key used in the KAEW can be flexible according to the combination of the block cipher and the stream cipher. Therefore, the KAEW can be applied for both binary mode and the text mode which is similar to the OTP. Thus, it is easy to be implemented in both hardware and software. Nevertheless, its cipher text is very difficult to be broken by hackers. Moreover, each block of the KAEW can have variable sizes depended on the length of the random number that generates from the sequenced key generator, that forces cryptanalyzers hard to guess the value of the random number if they have only the cipher text and the plaintext. So, the KAEW is tolerant to "chosen plaintext attack" and "chosen cipher text attack".

7. CONCLUSION

It is the fact that the secrecy of all plaintexts transferred over the Internet is critical. Therefore, the security issue has been concerned for decades but there is no best rule to fit the demand. Various techniques, such as DES, and AES, and OTP, have been proposed by researchers. However, only some of them have been implemented in the E-commerce system. Although OTP has been claimed to be the best method to encrypt the plaintext, its weak point is based on the length of the key and random numbers to be used. Therefore, this method has not been implemented, except the high security of the plaintext is really needed. Other methods also have their limitations, such as size of the block cipher, size of the key, including the mode of the plaintext to be applied.

According to limitations of available methods mentioned above, the plaintext still post security threat. Therefore, this paper proposed a chain rule mechanism called the KAEW to create a set of a cipher text from a set of an input stream. This method has delimited all limitations from existing mechanisms since its implementation is based on the concept of the best cipher mechanism, OTP. However, the KAEW has its significant characteristics that the length of the main key can be flexible, much shorter than the original OTP rule while the secrecy of the plaintext is still reserved. Moreover, the randomness problem of OTP does not exist in this algorithm since the seed number will be changed from time to time. Additionally, the mode to perform the encryption mechanism can be either binary mode or text mode; this causes much flexible to be implemented in hardware and software.

8. REFERENCES

[1] Behrouz A. Forouzan, *Introduction to Cryptography and Network Security international Edition*, McGraw Hill, New York, USA, 2008.

[2] J. Talbot, D. Welsh, *Complexity and Cryptography An Introduction*, Cambridge University Press, United States of America by Cambridge University Press, New York, 2006.

[3] NIST FIPS PUB 46-3, *Data Encryption Standard. Federal Information Processing Standards, National Bureau of Standards*, U.S. Department of Commerce, Washington D.C., 1977.

[4] Willian J. Beyda, *Data Communications from Basics to Broadband third edition*, Prentice Hall, New Jersey, USA, 1997.

[5] Behrouz A. Forouzan, *Data Communications and Networking fourth Edition*, McGraw Hill, New York, USA, 2007.

[6] KT Ng, WN Chau, and YM Siu, "An Internet Security System for E-commerce", *IECON 02 Industrial Electronics Society, IEEE 2002 28th Annual Conference of the*, Nov. 5-8, 2002,
vol.3, pp. 2468 - 2472.

[7] B. Schneier, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc, Hoboken, New Jersey, USA, 1996.

[8] National Institute of Standards and Technology: Advanced Encryption Standard (AES) web site: "crsc.nist.gov/encryption/aes".