JASEM ISSN 1119-8362
All rights reserved
Full-text Available Online at
https://www.ajol.info/index.php/jasem
http://ww.bioline.org.br/ja
J. Appl. Sci. Environ. Manage.
Vol. 22 (8) 1193 –1197 August 2018

Replication of Ciphertext in Cryptographic System

OSAGHAE, E O

Department of Computer Science, Federal University, Lokoja, Kogi State, Nigeria.
Email: edgarosaghae@gmail.com

ABSTRACT: Eavesdroppers are constantly trying to reveal encrypted messages sent within communication channels. The motive to illegally decrypt ciphertexts (encrypted messages) could be for economical, security or political reasons. Finding secured way of protecting ciphertexts from being stolen and revealed, has been very challenging for existing cryptographic researchers. This paper proposes a novel method to protect the ciphertext by replication the original plaintext (unencrypted messages) by altering them before encrypting them and then send the ciphertexts through the communication channel. In the communication channel, if an eavesdropper attempt to intercept the ciphertext, the listener is subjected to large range of guesses, of which ciphertext is the right one to perform cryptanalysis. When the Eavesdropper is subjected to large range of guess work, the process of cryptanalysis is made more difficult. Increasing the difficulty in cryptanalysis as a result of subjecting the Eavesdropper to large range of guessing is believed to be a promising technique of securing a message in a cryptographic system.

DOI: https://dx.doi.org/10.4314/jasem.v22i8.8

Dates: Received: 10 July 2018; Revised: 19 August: 2018; Accepted: 26 August 2018

Keywords: Eavesdropper, Encryption, Decryption, Ciphertext, Plaintext, Cryptanalysis

In our modern age of telecommunications and the Internet, information has become a precious commodity. Sometimes, it must therefore be keep safe from stealing by an eavesdropper. One essential feature for secure communications is through the use of cryptography, which not only protects data from stealing or modification, but can also be used for user authentication. The main aim of cryptography is to protect data transferred in the likely presence of enemies. A cryptographic transformation of data is a procedure by which plaintext data is encrypted, resulting in a modified text, called cipher text, that does not expose the original input. The cipher text can be reverse-altered by a designated recipient so that the original plaintext can be recaptured. There are two main fields of modern cryptographic techniques: Public key encryption and Secret key encryption. A public-key encryption is a process whereby a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. A secret key is an encryption key known only to the party or parties that exchange secret messages. The risk in this system is that, if either party loses the key or it is stolen, the system is broken (Payal and Soni, 2014).

Cryptography, the science of encrypting and decrypting information, was invented in 1900 BC, when a scribe in Egypt first used a derivation of the standard hieroglyphics of the day to communicate. There are many notable personalities who participated in the evolution of Cryptography and they are, Julius Caesar (100-44 BC); used a simple substitution with the normal alphabet in government communications, and later, Sir Francis Bacon; in 1623, who described a cipher that is known today as a 5-bit binary encoding. For all the historical personalities involved in the evolution of cryptography, it is William Frederick Friedman, founder of Riverbank Laboratories, who was a cryptanalyst for the US government, and lead code-breaker of Japan's World War II Purple Machine. In 1918, Friedman authored The Index of Coincidence and Its Applications in Cryptography, which is still considered by many in this field, as the premiere work on cryptography written this century. During the late 1920s and into the early 1930, the US Federal Bureau of Investigation (FBI) established an office designed to deal with the increasing use of cryptography by criminals (Govinda and Sathiyamooth, 2011; Jirwan et al., 2013). In the 1970s, Dr. Horst Feistel established the Data Encryption Standard (DES) with his family of ciphers called the Feistel ciphers, while working at IBM‟s Watson Research Laboratory. In 1976, two contemporaries of Feistel, Whitfield Diffie and Martin Hellman first

Email: edgarosaghae@gmail.com

introduced the idea of public key cryptography in a publication entitled: New Directions in Cryptography. Public key cryptography is what the existing industry standard, uses in its software. In the September, 1977 issue of The Scientific American, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman introduced to the world, their RSA cipher, applicable to public key cryptography and digital signatures. The authors offered to send their full report to anyone who sent them self-addressed stamped envelopes, and the ensuing international response was so overwhelming. In 1994, Professor Ron Rivest, co-developer of RSA cryptography, published a new algorithm, RC5, on the Internet. It had been claimed that RC5 is stronger than DES. Cryptography is used to achieve the following goals: *Confidentiality:* To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair. *Data integrity*: To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication codes or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered. *Authentication*: To assure that data originates from a particular party. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent (Govinda and Sathiyamooth, 2011).

Cryptography is the study of mathematical systems for solving two kinds of security problems: privacy and authentication. A privacy system prevents the extraction of information by unauthorized parties from messages transmitted over a public channel, thus assuring the sender of a message that, it is being read only by the intended recipient. An authentication system prevents the unauthorized injection of messages into a public channel, assuring the receiver of a message of the legitimacy of its sender. A communication channel is considered public if its security is inadequate for the needs of its users. A communication channel such as a telephone line may therefore be considered private by some users and public by others. Any communication channel may be threatened with eavesdropping or injection or both, depending on its use. In telephone communication, the threat of injection is paramount, since the called party cannot determine which phone is calling. Eavesdropping, which requires these of a wiretap, is technically more difficult and legally hazardous. Eavesdropping is passive and involves no legal hazard, while injection exposes the illegitimate transmitter to discovery and prosecution. In an authentication system, cryptography is used to guarantee the authenticity of the message to the receiver. Not only must a meddler be prevented from injecting totally new, authentic looking messages into a communication channel, but he must be prevented from creating apparently authentic messages by combining, or merely repeating, old messages which he has copied in the past. A cryptographic system intended to guarantee privacy will not, in general, prevent this latter form of mischief. To guarantee the authenticity of a message, information is added which is a function not only of the message and a secret key, but of the date and time as well; for example, by attaching the date and time to each message and encrypting the entire sequence. The first step in assessing the adequacy of cryptographic systems is to classify the threats to which they are to be subjected. The following threats may occur to cryptographic systems employed for either privacy or authentication. A ciphertext only attack is a cryptanalytic attack in which the cryptanalyst possesses only ciphertext. A known plaintext attack is a cryptanalytic attack in which the cryptanalyst possesses a substantial quantity of corresponding plaintext and ciphertext. A chosen plaintext attack is a cryptanalytic attack in which the cryptanalyst can submit an unlimited number of plaintext messages of his own choosing and examine the resulting cryptograms. Ciphertexts produced by a classical cipher (and some modern ciphers) always reveal statistical information about the plaintext, which can often be used to break them. After the discovery of frequency analysis perhaps by the Arab mathematician and polymath, Al-Kindi (also known as Alkindus), in the 9thcentury, nearly all such ciphers became more or less readily breakable by any informed attacker. Such classical ciphers still enjoy popularity today, though mostly as puzzles. Al-Kindi wrote a book on cryptography entitled Risalah fi Istikhraj al-Mu'amma (Manuscript for the Deciphering Cryptographic Messages), in which described the first cryptanalysis techniques (Diffie and Hellman, 1976; Al-Vahad and Sahhavi, 2011; Goyal, 2012; Pandey et al., 2013; Massey, 1988).

There are some researchers who have attempted to substantially improve on the use of cryptography to secure messages sent through public communication channels. The review of existing literature stated with the work of in (Pandey et al., 2013), whereby the

authors improved on security of messages sent through a communication channel, by using the enhanced symmetric key encryption algorithm. The algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. The algorithm use key size of 512 bits for providing better security and it also provide the concept of internal key generation at receiver end on the basis of 512 bits key which will entered by the sender. Advantages of the algorithm are: (i) Prevention ofbrute force attack and other harmful attacks on security, (ii) It is efficient for large data where existing algorithms provides efficient encryption and decryption only for 2MB data, (iii) This work provides better speed in comparison to existing algorithms for large size of files with less overhead, (iv) The proposed method for both encryption and decryption can be applied for any type of public application for sending confidential data and by sending internal key to the sender by using another secured path to the receiver. (v) Proposed method prevents data from attackers and claim for less time complexity with large data. So it provides useful application in the field of network security (Pandey et al., 2013).

Goswami and Singh (2012) investigated the existing security schemes and to ensure data confidentiality, integrity and authentication. They adopted symmetric and asymmetric cryptographic algorithms for the optimization of data security in cloud computing. These days encryption techniques which use large keys (RSA and other schemes based on exponentiation of integers) is seldom used for data encryption due to computational overhead. Their usage is restricted to transport of keys for symmetric key encryption and in signature schemes where data size is generally small. Public Key Cryptography with Matrices is a three-stage secured algorithm. They generated a system of non-homogeneous linear equations and using this system, they described algorithms for key agreement and public encryption, whose security is based on solving system of equations over the ring of integers which comes under the NP-Complete problems (Goswami and Singh, 2012).

Abikoye *et al* (2012) proposed a data hiding system that is based on audio steganography and cryptography to secure data transfer between the source and destination. Audio medium is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the audio file. The proposed system was evaluated for effectiveness and the result shows that, the encryption and decryption methods used for developing the system make the security of the proposed system more efficient in securing data from unauthorized access. The first advantage of this method is that it does not tamper with the original size of the file even, after encoding. The second advantage of this method is that encryption and decryption techniques used with this system, make its security more robust. The authors recommended the proposed method be used by the Internet users for establishing a more secure communication (Abikoye et al., 2012).

METHODOLOGY

In this section, there will be a description of how the proposed secured cryptographic system works. It will starts with a description of the architecture of the proposed secured cryptographic system, followed by the behaviour of secured cryptographic system.

Secured Cryptographic System: The proposed secured cryptographic system is an equivalent of the general cryptographic system that sends messages from many senders to many receivers. The only difference is an attempt of sending many messages to one receiver. Figure 1 shows architecture for securing a cryptographic system, by subjecting an eavesdropper to guess work, of which of the tapped available numerous ciphertexts is the correct one to perform cryptanalysis. When a sender wants to send a message to a receiver, he replicates the plaintexts to different fictitious messages, leaving only one of the messages unaltered. The proposed cryptographic system comprises of the following components: Sender, Receiver, altered replicated plaintexts (PT1, PT2, PT3,…,PTk,…,PTn), Encrypt, Ciphertexts (CT1, CT2, CT3,…,CTk,…,CTn), Decrypt(CTk and k), Plaintext (PTk), Eavesdropper (CT1, CT2, CT3,…, CTk,…CTn-1, CTn).

i) Sender: is the person with the intention of sending a message from one location to another, through an unsecured channel. The sender also has an available secured channel to send the decryption key and identification number of the correct ciphertext for decryption. The desire of the sender is to send a message to the Receiver without an Eavesdropper able to have access to it.

ii) Receiver: is the rightful owner of the message being sent. The aspiration of the sender is the assurance that he is the only person who has received the desired message that has not been altered during the sending process. The Receiver gets many fictitious messages, with only one correct unaltered message. The Receiver gets the identification number of the right Ciphertext message (CTk) and the decryption key (k).

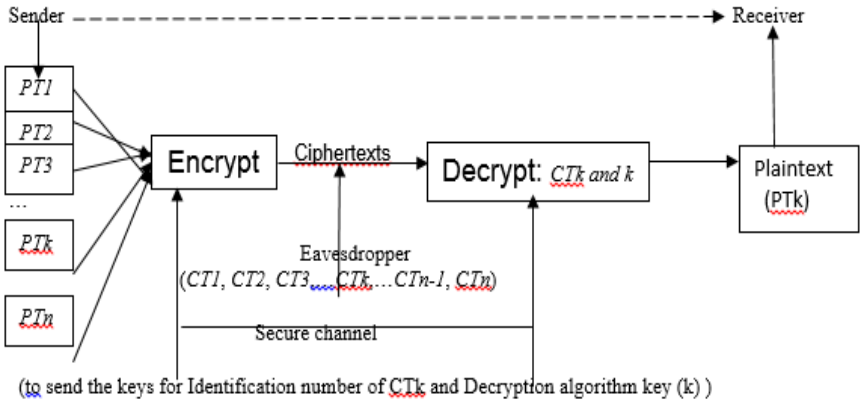

Fig 1: Architecture for Securing a Ciphertext

iii) Replicated plaintexts (PT1, PT2, PT3,…,PTk,…,PTn): is the set of altered replicated plaintext messages except one (PTk) that is altered and desired for the Receiver. These replicated plaintext messages are fed into the Encrypt section.

*iv) Encrypt***:** is the section responsible for encrypting the set of replicated Plaintext messages (PT1, PT2, PT3,…,PTk,…,PTn) prior to their transmissions through the unsecured channel. The Encrypt section also assist in sending the identification number of desired cipertext (ik) and Decryption algorithm key (k), through a secured communication channel.

*v) Ciphertexts (CT1, CT2, CT3,…,CTk,…,CTn)***:** is a set of encrypted messages that is altered and replicated with only one unaltered message (CTk).

vi) Decrypt (CTk and k): is a section that is responsible for identifying decrypting the correct Ciphertext (CTk) and using the decryption key (k). Both the correct Ciphertext (CTk) identification and the decryption key (k) are sent to the decryption section through a secured communication channel.

vii) Plaintext (PTk): is the correct message that is the only unaltered plaintext. When this desired plaintext is decrypted and retrieved from the Decrypt section, it is sent to the Receiver, who is the owner of the message.

Behaviour of Secured Cryptographic System: The behaviour of secured cryptographic system starts from when a sender intends to send a message through an unsecured communication channel to a receiver. The sender sends the plaintext PTk, but first has to replicate the plaintext messages using but leaving one of the messages unaltered (PTk). The replicated plaintext messages are PT1, PT2, PT3,…,PTk,…PTn. Where plaintext, PTk is the correct plaintext and n is the number of plaintext generated to be transmission across a communication channel. The set of replicated messages are sent to the Encrypt section. The Encrypt section is responsible for encrypting all the replicated plaintext messages into Ciphertexts (CT1, CT2, CT3, …,CTk,…,CTn-1, CTn). The encryption of a plaintext PT1, PT2, PT3,…,PTk,…PTn are the ciphertext e_k(PT1, PT2, PT3,…,PTk,…PTn). Where k is the key and t is the identification number of the correct ciphertexts CTk. The keys of other ciphertexts except CTk are not given because they will not be decrypted at the receiver end of the cryptographic system and hence, there is no need to generate them. These Ciphertexts are sent through unsecured communication channel, while the identification number for t and its decryption algorithm key (k) is sent through a secured communication channel. The Ciphertexts are replicated with only one of them that is correct, is to subject a suspected Eavesdropper to more guess work, in case he have access to the set of replicated Ciphertexts. The problem created for the Eavesdropper is which of the Ciphertexts is the correct one to perform cryptanalysis upon. The main function of the Decrypt section is to identify only the correct Ciphertext (CTk) using its identification number (t) sent through a secure communication channel. When the desired Ciphertext (CTk) is retrieved, others are discarded and the key (k) is used to decrypted the ciphertext. When the replicated Ciphertexts arrived at their destination, they are submitted to the Decrypt (CTk and t) section. The decryption function is $e^{-1}{}_k$:$e^{-1}{}_k$(CT1, CT2, CT3, …,CTk,…,CTn-1, CTn) = $e^{-1}{}_k$ (e_k (PTk)) = PTk = desired plaintext. After the desired plaintext (PTk) has been retrieved from the decrypt section, it is sent to the Receiver.

RESULTS AND DISCUSSION

The proposed secured cryptographic system is aimed to subject a suspected eavesdropper to large range of guessing of the ciphertexts messages that is the real one. Before now, the eavesdropper only has to worry about how to decrypt a particular ciphertext message

however, with the introduction of replicating the ciphertext will compound the problem for the eavesdropper. If the eavesdropper succeeds in capturing a victim's ciphertext, he/she may likely have the wrong ciphertext. For instance, when there is an attempt to decrypt the wrong ciphertext, it will lead to wasteof efforts and tine of the eavesdropper. This proposed technique has added another layer of security for messages sent from a source to destination. The proposed technique will not incur additional process of decrypting more than one ciphertext message for the receiver of the message because, only the right ciphertext message (CTk) is decrypted. The receiver of ciphertext messages, attempts to decrypt only the right message using the identification number of the ciphertext message, other fooling ciphertext messages are discarded from the system. The existing improvement techniques of the existing cryptographic techniques, focused on securing a particular ciphertext message sent through an unsecured public communication channel. The introduction of this novel cryptographic technique will further lengthy the cryptanalysis process of an eavesdropper and even if he/she is determine to decrypt a ciphertext message, the decryption process is made complicated.

Conclusion: Although, this paper proposes a novel cryptographic technique that will improve security of ciphertexts, a drawback is that the ciphertexts generated during the replication stage increases the contents of messages in the communication channel. Future direction of this research work is to apply data compression technique on the replicated ciphertexts, and conduct performance evaluation on the load effect on the communication channel.

REFERENCES

Abikoye O. C; Adewole K. S; Oladipupo A. J (2012). Efficient Data Hiding System using Cryptography and Steganography, *Inter. J. Appl. Information Sys.* 4(11): 6-11.

Al-Vahad A; Sahhavi H (2011). An Overview of Modern Cryptography, *World Appl. Programming*, 1(1): 55-61.

Diffie W; Hellman M. E (1976). New Directions in Cryptography, *IEEE Transact. Info. Theory*, 22(6):644-654.

Goswami B; Singh S. N (2012). Enhancing Security in Cloud Computing using Public Key Cryptography with Matrices, *Inter. J. Engineer. Res. Applica.*2 (4): 339-344.

Govinda K;Sathiyamooth E (2011). Multilevel Cryptograpy Technique Using Graceful Codes, *J. GlobalRes. Comp. Sci.* 2(7): 1-5.

Goyal S (2012). A Survey on the Applications of Cryptography, *Inter. J. Sci. Technol.* 1(3): 137-140.

Jirwan N; Singh A; Vijay S (2013). Review and Analysis of Cryptography Techniques, *Inter. J. Sci. Engineer. Res.* 4(3): 1-6.

Massey J. L (1988). An Introduction to Contemporary Cryptology, *Proceedings of the IEEE*, 76(5): 533-549.

Pandey K. K; Rangari V; KumarSinha S (2013). An Enhanced Symmetric Key Cryptograpy Algorithm to ImproveData security, *Inter. J. Comp. Applica.*74 (20): 29-33.

Payal P. P; Soni P. D (2014). Quantum Cryptography: Realizing next generation in Information Security. *Inter. J. Applica. Innov. Engineer. Manage.*3 (2): 286-289.