2nd International Conference on Emerging Trends in Engineering, Science and Management
Indian Federation of United Nations Associations, New Delhi (India) (ESM-17)
13th August 2017, www.conferenceworld.in ISBN: 978-93-86171-59-7

Repeated Random Enciphering – A Novel Method to Support Data Security on Transit over Networks

Dr. D. I. George Amalarethinam [1] and P. Muthulakshmi [2]

[1] *Jamal Mohamed College (Autonomous), Tiruchirapalli, (India)*

[2] *SRM University, Kattankulathur Campus, Chennai, (India)*

ABSTRACT

The growth of network of computers has paved way for the ease of communication and the benefits of networks can be listed to a great extent. The growing need for network security and secure data transfer has to be focused in parallel. The most common tool for providing network security is cryptography. In this paper, we proposed an algorithm, which could speak the need on new and advanced encryption standards for the future. In our work, we proposed an idea to encrypt the plain text, which performs various transformations and generating random numbers and random operators on the plain text. The process of decryption takes the cipher text and the secret key to produce the original plain text. The encryption is done at regular intervals of time and previously generated encoded message is allowed to disperse and cannot be seen any more. The process of encryption is happening repeatedly and hence it not easy to trap the contents at any point of time. The encrypted message will be of computer integers assorted with the random numbers generated by the randomizer after some basic mathematical operations done. The mathematical operations are chosen random from a list of operations. The algorithm is implemented in Java and is found giving better results.

Keywords - Cryptography, Decryption, Encryption, Randomizer, Network Security

I. INTRODUCTION

From the dawn of civilization, to the highly networked societies that we live today, communication has always been an integral part of our existence. Simple sign-communication followed centuries ago have evolved into many forms of communication today. Methods of communication today include radio communication, telephonic communication, network communication, mobile communication. All these methods and means of communication have played an important role in our lives, but in the past few years, network communication, especially over the internet, has emerged as one of the most powerful methods of communication. The rapid advances in communications technology have also given rise to security threats to individuals and organizations. In the last few years, various measures and services have been developed to counter these threats. All categories of such measures and services, however, have certain fundamental requirements, which include confidentiality, authentication, integrity, non-repudiation. Confidentiality is the process of keeping information private and secret and therefore only the intended recipient is able to understand the information. Authentication is the process of providing proof of identity of the sender to the recipient and that the recipient can be assured that the person sending the information is who and what he or she claims to be. Integrity, which is the method to ensure that information is not tampered during its transit or storage on the network. Any unauthorized person should

not be able to tamper the information or change the information during transit. Once the non-repudiation process is in place, the sender cannot deny being the originator of the data. The idea in this paper ensures the secure delivery of the message or text, when send between computers in the network.

II. CRYPTOGRAPHY

Cryptography[1] is the science of protecting data, which provides means and methods of converting data into unreadable form, so that the data cannot be accessed by unauthorized use. The other aspects of cryptography are: (1) the content of the data frames is hidden, (2) the authenticity of the data can be established, (3) the undetected modification of the data is avoided, (4) the data cannot be disowned by the originator of the message. Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. Cryptography is especially useful in the cases of financial and personal data irrespective of the fact that the data is being transmitted over a medium or is stored on a storage device. It provides a powerful means of verifying the authenticity of data and identifying the offender, when the confidentiality and integrity of the data is violated. Because of the development of electronic commerce, cryptographic techniques are extremely critical to develop and to use such technique to defend against attacks. The method of encryption was known as substitution cipher. In this method, each letter of the clear text message shall be replaced by some other letter, which results in an encrypted message or cipher text. The method works as,

The clear text message: WELCOME

The cipher text message (encrypted by using substitution cipher): XFMDPNF

In the above example, each letter of the plaintext message has been replaced with the next letter in the alphabet. This type of substitution is also known as Caesar cipher. Caesar cipher is an example of shift cipher because it involves shifting each letter of the plaintext message by some number of characters on the sequel of alphabets to obtain the cipher text. However, simple substitution ciphers are not a very reliable and can easily be broken down. In such a case, an alternative way is to use multiple alphabets instead of one alphabet. This type of a cipher, which involves multiple cipher alphabets is known as a poly-alphabetic substitution cipher. With the recent advances in mathematical techniques, there is an acceleration in the development of new methods of encryption. Today, cryptography has emerged so powerful that it is considered rather impossible to break some ciphers. Cryptography has now become an industry standard for providing information security, trust, controlling access to resources, and electronic transactions. Its use is no longer limited to just securing sensitive military information. In fact, cryptography is now recognized as one of the major components of the security policy of an organization.

III. TYPES OF SECURITY ATTACKS

One of the most important methods that provide security to messages on its transit is cryptography. It helps overcoming the security issues as described section 2 also, it is involved in the delivery of messages over any communication channel. Some of the types of security attacks are as follows,

Interruption: In an attack, where one or more of the systems of the organization become unusable due to attacks by unauthorized users which may lead to systems being unavailable for use.

Interception: An unauthorized individual intercepts the message content and changes it or uses it for malicious purposes. After this type of attack, the message does not remain confidential

Modification: A third party may modify the content of the message. This attack affects the integrity of the message.

Fabrication: In this attack, a third party inserts spurious messages into the organization network by posing as a valid user. This attack affects the confidentiality, authenticity, and integrity of the message.

IV. TERMS INVOLVED WITH CRYPTOGRAPHY

This section of the paper discusses on terms that are essentially be known before getting into the thick of cryptography,

Plaintext: the message that has to be transmitted to the recipient, also commonly referred as clear text.

Encryption: the process of changing the content of a message that may hide the actual message.

Cipher text: the output that is generated after encrypting the plain text.

Decryption: the reverse of encryption and is the process of retrieving the original message from its encrypted form. This process converts cipher text to plaintext.

Hash algorithm: an algorithm that converts text string into a string of fixed length.

Key: a word, number, or phrase that is used to encrypt the clear text. In computer–based cryptography, any text, key word, or phrase is converted to a very large number by applying a hash algorithm on it. The large number, referred to as a key is then used for encryption and decryption.

Cipher: is a hash algorithm that translates plaintext into an intermediate form called cipher text, in which the original message is in an unreadable form.

Cryptanalysis: is the science of breaking codes and ciphers.

Cryptography techniques: the classification of encryption and decryption techniques are categorized on the basis of the number of keys that are used. The two main cryptography techniques are

Single key cryptography: This cryptography technique is based on a single key. It is also known as symmetric key or private key or secret key encryption.

Public key cryptography: This cryptography technique is based on a combination of two keys—secret key and public key. It is also known as asymmetric encryption.

4.1 Single Key Cryptography

The process of encryption and decryption of information by using a single key is known as secret key cryptography or symmetric key cryptography. In symmetric key cryptography, the same key is used to encrypt as well as decrypt the data. The main problem with symmetric key algorithms is that the sender and the receiver have to agree on a common key. A secure channel is also required between the sender and the receiver to exchange the secret key.

V. RELATED ALGORITHMS [3]

Many secret key algorithms were developed on the basis of the concept of secret key cryptography.

5.1 Data Encryption Standard (DES)

The most widely used secret key algorithms include Data Encryption Standard (DES). DES is still surrounded by controversy. This controversy was originally fueled by the following facts: The key length used by this algorithm was reduced to 56 bits by the U.S. government, although the original design called for a key length of 128 bits, leading to a compromise on security. Although the algorithm for DES was published, the rationale for the design was never published. DES became widely available to the U.S. public and to approved users in other countries. However, DES was excluded by the U.S. government from protection of any of its own classified information. The major weaknesses and attacks that are faced by DES are described as follows,

The simplest attack to decipher a DES key is the brute force attack. The brute force attack on the DES algorithm is feasible because of the relatively small key length (56 bit) and ever-increasing computational power of the computers. Until the mid-1990s, brute force attacks were beyond the capabilities of hackers because the cost of computers that were capable of hacking was extremely high and unaffordable. With the tremendous advancement in the field of computing, high-performance computers are relatively cheaper and, therefore, affordable. In fact, general purpose PCs today can be successfully used for brute force attacks. Many hackers today are using more powerful techniques, such as Field Programmable Gate Array (FPGA) and Application-Specific Integrated Circuits (ASIC) technology that provide faster and cheaper means of hacking. Any cipher can be broken by trying all keys that possibly exist. However, in brute force attacks, the time taken to break a cipher is directly proportional to the length of the key. In a brute force attack, keys are randomly generated and applied to the cipher text until the legitimate key is generated. This key decrypts the data into its original form. Therefore, the encryption key length is a major factor that needs to be considered while choosing a key. The longer the encryption keys, the stronger the security. For example, in case of a 32-bit long key, the number of steps required to break the cipher are about 232 or 109. Similarly, a 40-bit key requires about 240 steps. This is something which can be achieved in one week by anyone sitting on his personal computer. A 56-bit key is known to have been broken by professionals and governments by using special hardware in a few months time. Today, 128-bit encryption is considered to be the safest and most reliable means of encrypting messages.

5.2 Triple Data Encryption Standard (3DES)

Triple-DES is a minor variation of DES. Although, three times slower than DES, it can be much more secure, if used properly. In today's scenario, Triple-DES is implemented more widely than DES. This is because DES is easy to break with the help of advanced technology that is widely available today. On the other hand, 3DES has proved to be an extremely reliable solution because of the longer key length that it uses. This extended length of key plays an important role in eliminating many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.

5.3 International Data Encryption Algorithm (IDEA)

The International Data Encryption Algorithm (IDEA) is a symmetric block cipher. It uses a 128-bit key to encrypt data in blocks of 64 bits. This is why it is referred to as a block cipher method. IDEA is designed to facilitate both software and hardware implementation. The major factors that make IDEA a strong algorithm are, (1) The key length is long enough to prevent comprehensive key searches. IDEA uses a key length of 128 bits, which makes it very secure. (2) The cipher text is not easily decipherable from the plaintext and the key. IDEA effectively masks the statistics of how the cipher text depends on the statistics of the plaintext. IDEA was developed to provide a high level of security with ease of implementation. Due to its strength and reliability IDEA is now used worldwide in many banking and industry applications.

5.4 RC4

RC4 is a cipher with a key size of up to 2048 bits (256 bytes). It is listed in the category of relatively fast and strong cipher methods. It is a stream cipher that creates a stream of random bytes and XORs these bytes with the text. Using RC4 with the same key on two different messages makes it very weak. It is thus useful in situations, in which a new key can be chosen for each message.

5.5 RC5

RC5 is yet another block cipher. Along with a variable key size, and a variable number of rounds, the size of RC5 data blocks is variable. The block size can range from 32 bits, 64 bits, to 128 bits. Similarly, the number of rounds can range from 0 to 255, while the key can range from 0 bits to 2040 bits in size.

5.6 CAST-128

This algorithm uses a variable key length and uses block sizes of 64 bits. The key lengths supported by CAST-128 vary from 40 bits to 128 bits, in increments of 8 bits. For key sizes that range up to 80 bits, the data block undergoes 12 rounds of encryption, while for key sizes of more than 80 bits, the algorithm has 16 rounds. For the keys whose sizes are less than 128 bits, zeroes are added to the rightmost (or the least significant) bits until the total length of the key result is 128 bits. This is done because the algorithm must have an input key of 128 bits in length. CAST-128 has shown very good encryption/decryption performance. Its implementation has processed up to 3.3 MB/sec on a 150 MHz Pentium processor.

5.7 Advanced Encryption Standard (AES)

With an estimated growth rate of two times every 18 months, computational power is growing in leaps and bounds. This has made Data Encryption Standard (DES) more and more insecure and vulnerable to malicious attacks. As a result, DES, which was the Federal Information Processing Standard (FIPS) until recently, has slowly become redundant. The National Institute of Standards and Technology (NIST) realized this situation and recognized the need for another standard that would be more secure than the DES. However, since DES is a federal standard, it is used widely by many organizations, particularly those in the financial industry. Advanced Encryption Standard (AES) emerged as a powerful replacement of DES during a competition held by NIST. The

competition was organized to develop a substitute of existing DES. The following algorithms reached the final round of the competition to become AES: MARS, RC6, Twofish, Serpent, Rijndael.

5.8 Problems in symmetric cryptography

The major problem with symmetric cryptography is that the process of transferring keys to the recipient is problem to security risks. Transferring the secret key over the Internet either in an e-mail message or through simple IRC services is insecure. Verbally communicating the key over a phone line runs the risk of eavesdropping. Similarly, snail mail runs the risk of possible interception. The security risks that are involved in secret key cryptography have been overcome to a large extent in another method of cryptography called public key cryptography. Public key cryptography uses a key pair instead of just one secret key. Of this key pair, one key, known as the private key, is always kept secret by the key holder. This private key is not transferred to anyone and is stored securely by the holder of the key and thus public key cryptography eliminates the need for transferring the private key. This not only solves the problem of key distribution but also makes the process of key management a lot simpler. In addition to this, public key cryptography also provides data integrity, authentication, and non-repudiation. Public key encryption can also be used for creating digital signatures, which are used for user authentication.

5.9 Public key cryptography

The approach called asymmetric cryptography evolved to address the security issues posed by symmetric cryptography. This method solves the problem of secret key cryptography by using two keys instead of a single key. Asymmetric cryptography uses a pair of keys. In this process, one key is used for encryption, and the other key is used for decryption. This process is known as asymmetric cryptography because both the keys are required to complete the process. These two keys are collectively known as the key pair. In asymmetric cryptography, one of the keys is freely distributable. This key is called the public key and is used for encryption. Hence, this method of encryption is also called public key encryption. The second key is the secret or private key and is used for decryption. The private key is not distributable. This key, like its name suggests, is private for every communicating entity. In public key cryptography, the data that is encrypted with the public key can only be decrypted with the corresponding private key. Conversely, data encrypted with the private key can only be decrypted with the corresponding public key. Due to this asymmetry, public key cryptography is known as asymmetric cryptography. This method very clearly indicates that the data send to a user can only be encrypted by the public key. Similarly, the decryption can be done only by the private key, which is supplied by the recipient of the data. So, there is very little possibility of the data in transit being accessed or tampered by any other person. Therefore, messages can be exchanged securely. The sender and receiver do not need to share a key, as required for symmetric encryption. All communications involve only public keys, and no private key is ever transmitted or shared. The above mechanism also brings out the point that every recipient will have a unique key that he will use to decrypt the data that has been encrypted by its counterpart public key. One of the most common implementations of this process is the RSA algorithm.

5.10 RSA

RSA refers to a particular implementation of public key cryptography; RSA has become the de facto standard in this field, to the point that RSA and public key encryption are often used as synonyms. In a cryptographic system with public keys, each object, person or party, must own one public key, which is publicly accessible to all other parties, and one private key, which must be kept secret. Hence, global communication requires only 2n keys, where *n* is the number of users. The procedure for the sending of a message from User A to User B is performed in the following way:

- User A obtains the public key of User B from a publicly accessible, authoritative place.
- User A then encrypts its message using this public key.
- User B receives the message and decrypts it with his/her private key.

RSA offers a few advantages that have helped in the achievement of manageable and more secure transactions. These advantages include 1. Simplification of the problem of key management: In symmetric encryption the number of keys required to allow *n* entities to communicate is proportional to *n2*. Whereas in asymmetric encryption each participant needs two keys; therefore, the total number of keys required is simply *2*n*. The growth in the number of keys with the growth in the number of users is linear and therefore manageable even when there are a large number of users. 2. Enhanced security of the transactions: Not only is the number of keys greatly reduced but the security offered by these keys is highly increased. Every user must have a pair of keys that he/she generates for himself/herself. The secret key must not be shared with anyone and so the problem of transmitting it does not arise, nor do the problems of secure channels and their management; the secret key really is secret, since it is shared with nobody. The public key, however, is shared with everyone, for example in a catalog, which it can be transmitted using the most convenient method, and therefore does not pose any problems regarding its privacy. RSA has now become an industry standard for encryption. In fact, such is the strength of RSA that the U.S. government has restricted its export to foreign countries.

5.11 Possible attacks on RSA

The RSA algorithm, although widely prevalent, has some weaknesses. Some of the common attacks that could be faced by RSA are, A) Factoring of the public key: At present RSA seems to be extremely secure. It has survived over 20 years of scrutiny and is in widespread use throughout the world. The attack that is most often considered for RSA is the factoring of the public key. If this can be achieved, all messages written with the public key can be decrypted. B) Cycle attack: In this attack, the cipher text is decrypted repeatedly, until the original text appears. A large number of recycles might be able to decrypt any cipher text. Again, this method is very slow, and for a large key it is not a practical attack. In spite of all the weaknesses of RSA, it continues to be regarded as a de facto industry standard for encryption, especially data transmitted over the Internet.

5.12 Combining Techniques: Symmetric and Asymmetric Encryption

The disadvantage of using public key encryption is that it is a slow process because key lengths are large (1024 bits to 4094 bits). When comparing both processes, secret key encryption is significantly faster as the key length is less (40 bits to 256 bits). On the other hand, there is a problem in transferring the key in secret key encryption. Both these techniques can be used together to provide a better method of encryption. The combined advantages and distance of the disadvantages. The steps in data transaction in a combined technique are:

1. Encrypt the file by using a symmetric encryption.
2. Use asymmetric encryption to encrypt only this key using the recipient's public key. Now send the encrypted key to the recipient. The recipient, at his end, can now decrypt the key using his/her private key.
3. Next, send the actual encrypted data. The encrypted data can be decrypted using the key that was encrypted by using the public key from the asymmetric key pair.

The combined technique of encryption is used widely. It is basically used for Secure Shell (SSH), which is used to secure communications between a client and the server and PGP (Pretty Good Privacy) for sending messages. Above all, it is the heart of Secure Sockets Layer (SSL), which is used widely by Web browsers and Web servers to maintain a secure communication channel with each other.

VI. PROPOSED WORK

The model for network security shows how the message is to be transferred from one party to another across wired or wireless medium via the internet. The two parties, who are the prime components in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP). Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

• A security-related transformation on the information to be sent, which include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a secret code based on the contents of the messages, which can be used to verify the identity of the sender.

• Some secret information shared by the two compoents. It is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

6.1 Need for encipherment algorithm

The goals of security can be threatened by security attacks. Snooping and traffic analysis of attacks threaten the confidentiality of information. The integrity of data can be threatened by modification, masquerading, replaying and repudiation. Denial of Service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system. The attack might intercept and delete a server's response to a client, making the client to believe that the server is not responding. The attacker may also intercept request from the client, causing the clients to send request many times and overload the system. The process of Encipherment mainly used for the protection of sensitive data. The implemented Data Encryption Standard (DES) and other proprietary symmetric block ciphers achieve confidentiality and integrity of messages. A data flow rate of more than 20 Mb/s makes is well-suited for local area networks or hard disk controller applications, the general encipherment scheme is proposed for files maintained in a paged structure in secondary storage. In addition, the effect of encipherment on file access and update, on paging mechanisms, and on files related to the enciphered index.

6.2 Random number generations

Random number generation play an important role in the use of encryption for various network security applications. These are pseudo random numbers which will support the uncertainty about the key. The generation of random numbers followed the uniform distribution.

6.3 Java Virtual Machine

Network is a domain of various machines run on a variety of CPUs under varied environments. It is found that Java would be better to implement the algorithm as Java supports the features of platform independency, portability, dynamic message passing, Unicode conversion, bytecode security by providing the firewall between the networked application and the personal computer [4].

6.4 How the algorithm works?

A. Encryption part of the algorithm

The process of encryption accepts the message as input a stream of data, converts it as a sequence of integers and allows to mix up with integers (random numbers) generated by the randomizer[4]. The mix up is the procedure where the sequence of integers is allowed to take some basic mathematical operations to be chosen by the randomizer. Hence, a random computation is done on random integers. Finally, the procedure returns the encrypted message collectively called the secret key. This process is continued with regular intervals of time. Hence, the encryption is done as dynamic procedure. There cannot be any stand point in the algorithm and that it is not easy for the intruder to trap the key.

B. Decryption part of the algorithm

The encrypted message has to be decrypted to view the original text. The reverse operation is carried out to get the original text.

6.2 Methodology of the proposed work

Randomness is a great utility that supports hiding information also the probability of hacking such randomly generated key is found null. As everything is done through random concept, the intruder cannot find very easy to trace. The memory occupied while transforming the original to the encrypted form is very less as when compared with the traditional algorithms. We use only the small integer (32 bits) for converting the message into its integer form and to generate the pseudo random numbers. The processing time of the algorithm is very less, since it involves with less operations. The vanishing of the encrypted text helps hiding the contents and no way allow the intruder to get the contents, just by tracking the encrypted message. The process of encryption is happening with regular intervals of time and the efficiency of algorithm is found better. Figure 1 illustrates the functioning of the proposed work.

Advantages

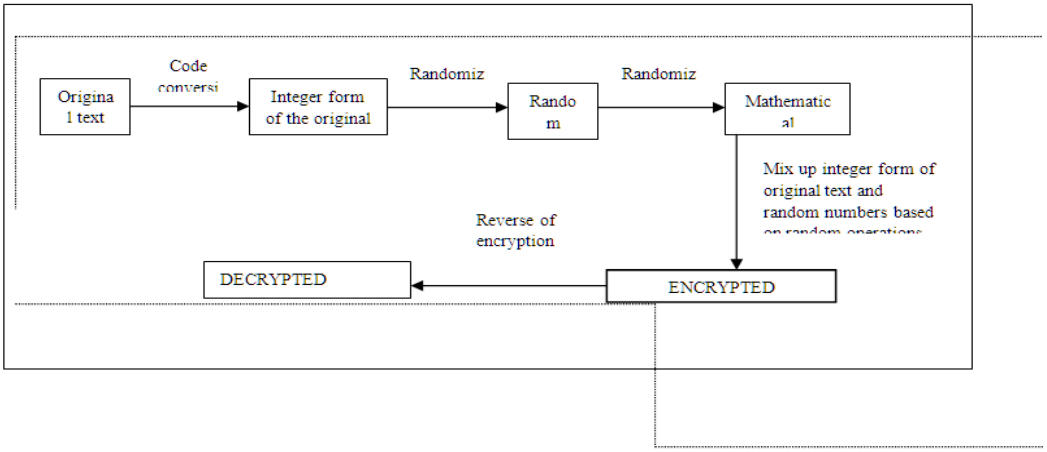

Figure 1. Random secret key generation

VII. CONCLUSION

The study of cryptography techniques will make us understand the need of security in web applications, like email, ecommerce, etc. Through this paper, an effort is taken to propose a new idea which ensures security mechanisms that avoids or considerably diminishes the threats The role of randomizer is very important to generate random numbers, operators and file names randomly to save the decrypted and encrypted messages. It is found better that the decrypted contents that repeatedly get decrypted in a stipulated period of time will protect the data from the attackers and it gives more security for the data. The proposed work may lead and encourage researchers to implement more concepts in the future. Also, we expect to explore the algorithm with images, sound data in future.

REFERENCES

[1] Behrouz A. Forouzen, "Cryptography and Network Security"

[2] Larryl Peterson, Bruce S. Davie, "Computer Networks a System Approach"

[3] William Stallings, "Cryptography and Network Security Systems"

[4] Herbert Schildt, "The Complete Reference JAVA"