A New Symmetric Key Algorithm for Modern Cryptography

Rupesh Kumar[1] Sanjay Patel[2] Purushottam Patel[3] Rakesh Patel[4]
[1,2]Students [3,4]Lecturer
[1,2,3]Department of Computer Science & Engineering [4]Department of Information Technology
[1,2,3,4]Kirodimal Institute Of Technology, Raigarh, Chhattisgarh, India

Abstract— Communication in any language between two or more persons is like a plaintext or simple text. That means any person knowing that language can easily understand this plain text until this plaintext is codified in some manner. So, it is important to implement the coding techniques to ensure that information is hidden from everyone for whom it is not intended. So, that only authenticated person will be allowed to access the information. Cryptography is the art and science of achieving security by the encoding of messages in an unreadable form. Cryptography derives from the Greek word; the word "crypto" comes from kruptos, which means "hidden" and graphy means "writing". Thus, Cryptography is the practice and study of the hiding messages. Today, the cryptography is considered as branch for both the Computer Science and mathematics, which will related to the information theory.

Keywords: Cryptography, Symmetric Key Algorithms, Network Security

I. INTRODUCTION

Today the whole world goes after the internet, which provides essential communication and information between thousands of people, and is being increasing in the aspects of the commerce, education, entertainment and many more. So, the security becomes an important issue to deal with it. There are many aspects to the security and many applications, ranging from secure commerce, payment to private communication and protecting password.

One important aspect towards the security is the Cryptography. The admiring concept of securing the messages through the cryptography has a historical record. In ancient times, When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3"rule could decipher his messages.

Cryptography is the science of using the concepts of mathematics to encrypt and decrypt the information; also it refers to art and science of designing the ciphers. Cryptography enables you to transmit or receive the sensitive information through an internet so that no one can access the information. Since, the cryptography is the science of securing the information, Cryptanalysis is the art and science of breaking the secure information and Cryptology involves both the cryptography and cryptanalysis. [1]Cryptographic algorithms and protocols can be grouped into four main areas:

- Symmetric encryption: Used to conceal the contents of streams of data of any size, including message files, encryption keys and password.
- Asymmetric encryption: Used to conceal the contents of stream of data, such as encryption keys and hash function values, which are used in digital signatures.
- Data integrity algorithms: Used to protect streams of data, such as message from alteration.
- Authentication protocols: These are schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities.

A Cryptographic algorithm is a mathematical functions used in the process of encryption and decryption. A cryptographic algorithm works in combination with a key – a word, number or phrase – to encrypt the plaintext. With the help of these keys this plain text is converted into ciphertext (an unreadable form). The security of the encrypted messages will depend up on the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. Without the use of decryption keys, the ciphertext cannot be converted into its plaintext.

There are two basic types of cryptography: Symmetric Key and Asymmetric Key. In symmetric (also called "private key") encryption, the same key is used for both encryption and decryption. In asymmetric (also called "public key") encryption, one key is used for encryption and another for decryption. A new Symmetric Key cryptographic algorithm has been proposed in this paper with its advantages

II. CRYPTOGRAPHY

The information can be read and understand without taking special steps will be considered as plain text. So it is necessary to hide the plaintext into some non- readable form. The process of hiding the contents of the plain text into some non-readable form i.e. ciphertext is called an encryption. The process of getting the plain text from the cipher text again is called the decryption as shown in figure.

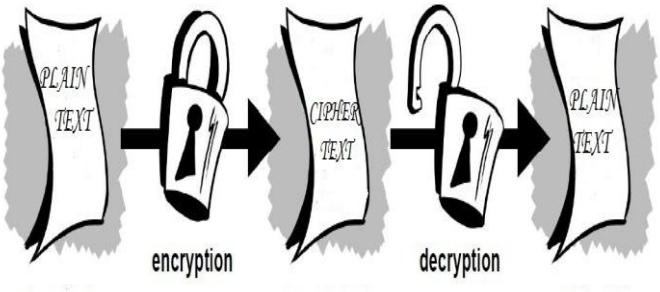

Fig. 2.1: Process of Encryption and Decryption

Generally, where cryptography is used, two parties (A and B) communicate over insecure channel (internet). They want to ensure that the exchange of information between them is secure or incomprehensible so that, anyone who might listening their conversation will not be able to understand. Since A and b are in remote locations, therefore

A also want to ensure that the information would not be modified by anyone (attacker) as the same information will be received by B as it is transmitted by A himself. Furthermore, B also want to ensure that the data should be transmitted by A not by anyone else. Thus, cryptography is used to achieve the following goals:

A. Data Confidentiality

With respect to the transmission of information over an unsecure channel i.e. internet, the information may not be secure. To ensure the security or privation of information during the transmission, the confidentiality of data should be necessary. Confidentiality is the protection of transmitted information from passive attackers. The data confidentiality can be achieved during the process of encryption. Encryption is the process of converting the plain text into cipher text. The security of data depends up on the strength of the encryption algorithm and the secrecy of the key and the equivalent decryption algorithm is used to convert the cipher text into plain text. In symmetric key algorithm only one key is used to encrypt or decrypt the text while in asymmetric key two different keys are used to encrypt or decrypt the text.

B. Data Integrity

Integrity means to impose the sets of rules and regulations. As with data confidentiality, integrity can apply to a stream of messages or a single message. There are two ways to impose the integrity: first one for connection oriented integrity service, if A send the stream of messages, and then he wants to ensure that the message will be received by B as sent, so that there will no modification, insertion, replays or duplications. The benefits of the integrity are that the destruction of data will be recovered. Second one for connectionless integrity service, one deal with individual messages without regard to any larger context, provides protection against only the modification. The verification of the integrity is done by the hash values. A hash value has a fixed length which is derived from the sequence of the data. To check the alteration of data, the hash values of the received data will be compared to the hash values of the data sent.

C. Authentication

The authentication is done to ensure that the communication or the exchange of the information is done by particular parties. The authentication should be provided by the digital certificate. In case of a single message, the role of the authentication service is to ensure the recipient that the message is from the source that it claims to be from. There are two types of specific authentication services are defined in X.800: (I) Peer entity authentication and (II) Data origin authentication.

D. Nonrepudication

The nonrepudication prevents either sender or receiver from denying the transmitted messages. Thus, when a message is sent by A, then the B can know that, A in fact transmitted the message to B. Similarly when a message is received by B, then the A can know that the B in fact received the message, by sending an acknowledgment data.

III. TYPES OF CRYPTOGRAPHY

Cryptography involves the process of scrambling the plaintext into the ciphertext and vice-versa. The process of conversion of plain text into cipher text is called an encryption and the process of conversion of ciphertext into plaintext is called decryption. There are several ways to classify the cryptographic algorithm, but there are two most successful algorithms: (I) Symmetric key cryptographic algorithm and (II) Asymmetric key cryptographic algorithm. In symmetric key cryptographic algorithm only one key is used to encrypt or decrypt the data, while in Asymmetric key cryptographic algorithm two different keys are used, one key is used for the process of encryption, and other will be used for the process of decryption. Figure 3.1 shows the types of the cryptographic algorithm.

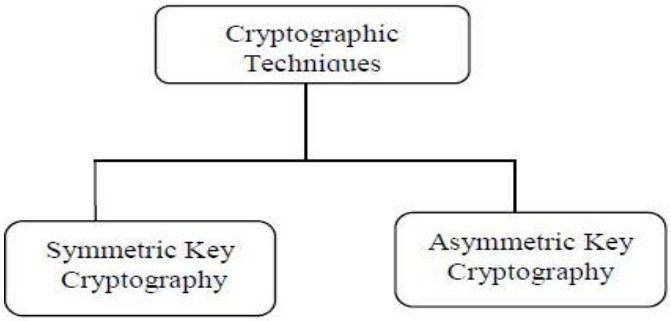

Fig. 3.1: Types of Cryptography

A. Symmetric key cryptography

It is also known as the secret key cryptography, in which only one key is used for both processes. The sender uses single key to encrypt the plaintext into the ciphertext, after the process of conversion of ciphertext from the plaintext. Then the receiver will use same key to decrypt the cipher text to get the plain text as shown in figure below. With this approach of the cryptographic algorithm the key should be known to both sender and receiver. The main disadvantage in this is the distribution of the key.

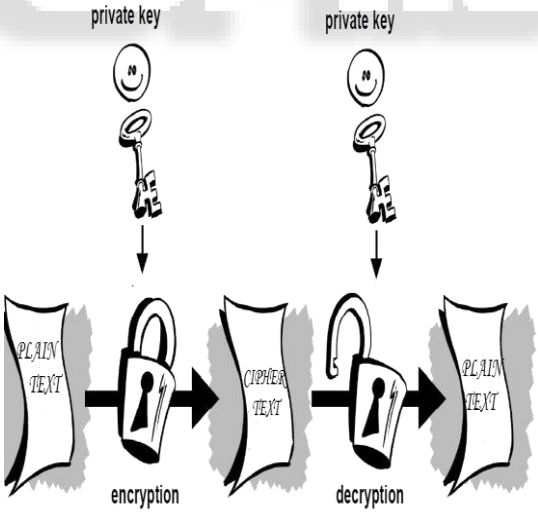

Fig. 3.1.1: Symmetric Key Cryptography

B. Asymmetric key cryptography

It is also known as a public key cryptography, in which two different keys are used to encrypt or decrypt the information, one key is used for the encryption process while the other one is used for the decryption process. In asymmetric key cryptography, the sender uses the public key for the encryption of the plain text, so that the other users will encrypt the data using the copy of the public key

but they are not allowed to decrypt it. The receiver has the private keys so that he can decrypt it as shown in below figure. The main advantages of using the asymmetric key are that allows the preexisting users to exchange the information securely.

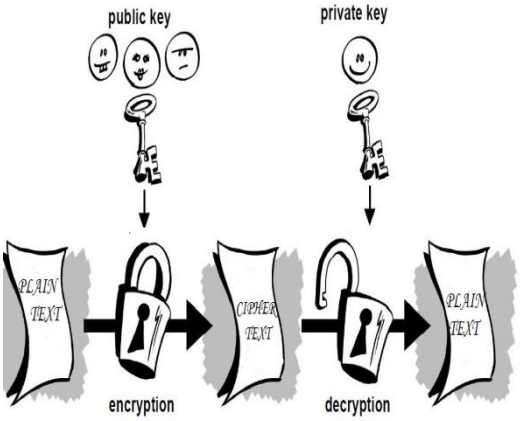

Fig. 3.2.1: Asymmetric Key Cryptographic

IV. SYMMETRIC KEY CRYPTOGRAPHY

Generally the private key cryptography or secret key cryptography is categorized as a block cipher or a stream cipher. A stream cipher is that which operates on the single bit or single byte at a particular time. In this approach, as shown in figure 4.1, the bit stream generator is a key controlled algorithm and produce a bit of stream i.e. cryptographically strong. The examples of the stream ciphers are the autokeyed vigenere and the vernam ciphers. A block cipher is that which operates on the block of the plaintext to produce a ciphertext block having equal length. Generally, a block size of 64 or128 bits will be used. As with a stream cipher, the two users share a symmetric encryption key, as shown in figure 4.2. Using some modes of operation, a block cipher can be used to achieve the same effect as a stream cipher.

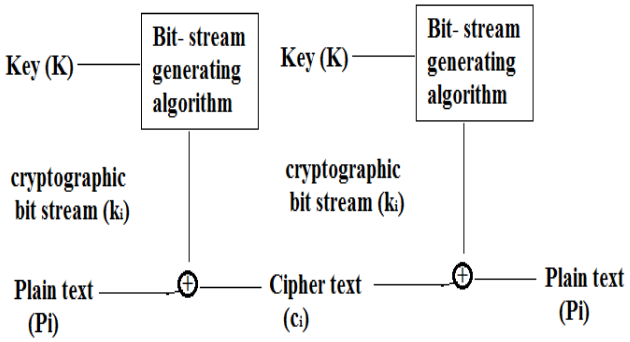

Fig. 4.1: Stream cipher using algorithm bit stream generator

[2]A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits. There are 2^n possible different plaintext blocks and for the encryption to be reversible (for decryption to be possible), each must produce a unique ciphertext block. Such a transformation is called reversible, or nonsingular.

Feistel proposed [FEIS73] that we can approximate the ideal block cipher by utilizing the concept of product cipher, which is the execution of two or more simple ciphers in the sequence in such a way that the final result or product is cryptographically stronger than any of the component cipher. The essence of the approach is to develop a block

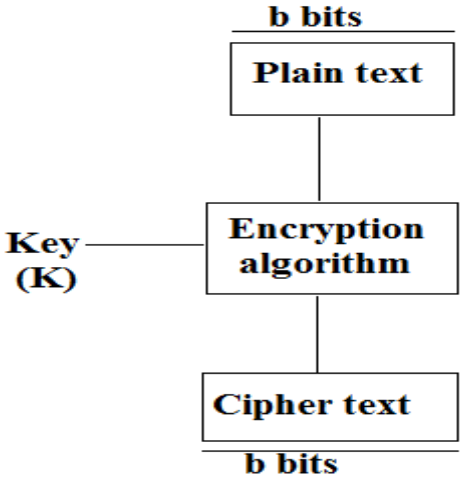

Fig. 4.2: Block ciphers

cipher with a key length of k bits and a block length of n bits, allowing a total of 2^k possible transformations. Generally, Feistel proposed the use of a cipher that alternates substitutions and permutations.

Substitution: Each letter of the plaintext is uniquely replaced by the corresponding ciphertext letters.

Permutation: A sequence of the plaintext letters is replaced by permutations of that sequence. That is, no letters are added or removed or replaced in the sequence.

V. KEYS

A key plays an important role in providing the security on the information transmitted over the unsecure channel. The key is value which will combines with the cryptographic algorithm in a plain text to produce a ciphertext. The security of data to be transmitted depends on the strength of the cryptographic algorithm and the secrecy of the key. If the has larger values, then the security will be more. Generally, there are two types of keys are used in cryptography: (I) Symmetric key and (II) Asymmetric key. In symmetric key cryptographic algorithm only one key is used to encrypt or decrypt the data, while in Asymmetric key cryptographic algorithm two different keys are used, one key is used for the process of encryption, and other will be used for the process of decryption.

Larger keys will be cryptographically secure for a longer period of time. In public key cryptography, the bigger the key, the more secure the ciphertext. While the public and private keys are mathematically related, it's very difficult to derive the private key given only the public key. Keys are stored in encrypted form. PGP stores the keys in two files on your hard disk; one for public keys and one for private keys. These files are called *key rings.*

VI. DIGITAL SIGNATURES

A digital signature provides an authentication mechanism which enables the writer of a message to attach a code that acts as a signature. The DSS (digital signature standard) is an NIST standard that uses the secure hash algorithm (SHA). A major benefit of the public key cryptographic is

that it provides a method of employing digital signatures. The different, as shown in figure 6.1`.The digital signature provides a set of security capabilities that would be difficult to implement in any other way.

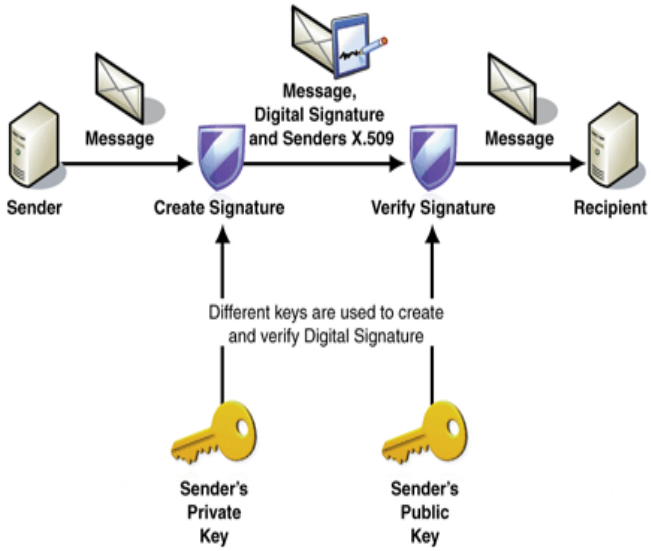

Fig. 6.1: Digital Signatures

The digital signatures has following properties:

- It must verify the author and the date and time of signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.

The digital signature has the following requirements:

- The signature must be bit pattern that depends on the message being signed.
- It must be relatively easy to produce the digital signature.
- It must be easy to recognize and verify the digital signature.
- It must be practical to retain a copy of the digital signature in the storage.

VII. New Proposed Symmetric Key Algorithm

This algorithm is easy to implement and more secure, because there is two reversed operations present in this algorithm which makes it more complex in nature. This algorithm is very easy to learn and practice because the steps followed in the process of conversion of the plaintext into the cipher text is very simple and vice-versa.

A. Encryption algorithm

As we know that the encryption is the process of conversing the plaintext into the ciphertext with the help of the cryptographic algorithm and the secret key. The steps followed in this algorithm are as follows:

Step1: Determine the ASCII value of the letter.

Step2: Determine the corresponding binary value of it. [Binary value should be 8 digits e.g. for decimal 32 binary number should be **00**100000]

Step3: Reverse the 8 digits of the binary value.

Step4: Take a 4 digits divisor (>=1000) as the **Key**.

Step 5: Divide the reversed number with the divisor.

Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the ciphertext i.e. encrypted text.

Now store the remainder in first 3 digits & quotient in next 5digits.

B. Examples

Let, the character is "T". Now according to the steps we will get the following:

Step 1: ASCII of "T" is 84 in decimal.

Step 2: The Binary value of 84 is 1010100. Since it is not an 8 bit binary number we need to make it 8 bit number as per the encryption algorithm. So it would be 01010100.

0	**1**	**0**	**1**	**0**	**1**	**0**	**0**

Step 3: Reverse of this binary number would be 00101010.

0	**0**	**1**	**0**	**1**	**0**	**1**	**0**

Step 4: Let 1000 as divisor i.e. Key.

Step 5: Divide 00101010 (dividend) by 1000(divisor).

Step 6: The remainder would be 10 and the quotient would be 101. So as per the algorithm the ciphertext would be 01000101 which is ASCII 69 in decimal i.e. "E".

0	1	0	0	0	1	0	1

C. Decryption algorithm

As we know that decryption is the process of conversing the ciphertext into plaintext using the private key. The steps followed in this algorithm are as follows:

Step 1: Multiply last 5 digits of the ciphertext by the Key.

Step 2: Add first 3 digits of the ciphertext with the result produced in the previous step.

Step 3: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number.

Step 4: Reverse the number to get the original text i.e. the plaintext.

D. Examples

After encrypting "T" we got 01000101 as the ciphertext. So, after decrypting this ciphertext into its plaintext, we have to get "T".

Now follow the steps of the decryption algorithm:

Step 1: After multiplying the last 5 digits of the ciphertext i.e. 00101 by 1000 (Key), the result would be 101000.

		1	**0**	**1**	**0**	**0**	**0**

Step 2: After adding 010 (first 3 digits of the ciphertext) with
101000 the result would be 101010.

		1	**0**	**1**	**0**	**1**	**0**

Step 3: Since 101010 is not an 8-bit number we need to make it 00101010.

0	**0**	**1**	**0**	**1**	**0**	**1**	**0**

Step 4: After reversing the number it would be 01010100 i.e.ASCII 84 in decimal i.e. "T" as character which was the original text.

0	1	0	1	0	1	0	0

E. Advantages

- This algorithm is easy to learn and implement.
- This algorithm is more secure because there will be two reverse operations in it which provides complexity.
- For small amount of data, this algorithm will be very useful because it takes less time to encrypt it.

VIII. CONCLUSION

To provide security of the information or the data confidentiality, or the data integrity, or the authentication, or the nonrepudilication, cryptography is the best method for implementing it. Since, cryptography is the art and science of hiding the original form into some other form. In order to achieve these goals, various cryptographic algorithms are developed. For a small amount of data or information to be encrypted, there should be efficient way to produce the ciphertext in a minimum cost. The main aim of this paper is to develop the new symmetric algorithm to produce the ciphertext for the small amount of information. By doing so, we can save our time and provide the security in data transmitted. As we know that the public key is more secure and advantages over the private key algorithm or the symmetric key cryptographic, therefore our next task is to find a new and simple public key cryptographic algorithm.

REFERENCES

[1] Cryptography and network security, 5th edition William Stallings
[2] Cryptography and network security, online publication, 5th edition William Stallings
[3] Computer and Network security by Atul Kahate.
[4] Fundamentals of Computer Security, Springer publications "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.htm#Algorithms.
[5] "A Brief History of Cryptography", by S. Hebert

