A SIMPLE SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHM

C.Chandrasekar[#], V.Prabhakaran [*]
#Assistant Professor, Sree Narayana Guru College, Coimbatore-11.
chandrasekar2000@gmail.com
**Assistant Professor, K.S.G College of Arts & Science, Coimbatore-15.*
prabhakaranmvp@gmail.com

Abstract-
Nowadays, the use of internet are growing increasingly across the world, security becomes a important issue for the society. A message in plain text can be understood by anybody knowing the language as long as the message is not codified in any manner. So, now we have to use coding scheme to ensure that information is hidden from anyone for whom it is not intended, even those who can see the coded data.

Cryptography is the art/science of achieving security by encoding messages to make them non-readable. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography ensures that the message should be sent without any alterations and only the authorized person can be able to open and read the message. Cryptography is used in applications include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

A number of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography- Symmetric key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. This paper describes cryptography, its principles, and its classification and then proposes a new symmetric key algorithm for both encryption and decryption with its advantages and limits over others.

Keywords
Cryptography, Symmetric Key, Asymmetric Key.

1. INTRODUCTION

In today's world where access to information in lesser time required with the goal of running the enterprise smoothly and efficiently, it is very important to give right people at right time. One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography plays a very vital role in keeping the message safe as the data is in transit. It ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptography embraces both cryptography and cryptanalysis.

"Cryptography" derives from the Greek word kruptos, meaning "hidden". The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key. The harder it is to discover the key, the more secure the mechanism. In symmetric (also called "secret-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.

Basic Terms Used in Cryptography

- **Plain Text**
  The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text.
- **Cipher Text**
  The message that cannot be understood by anyone or meaningless message (unreadable format) is what known as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message.
- **Encryption**

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption techniques to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

- **Decryption**

  A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption.

- **Key**

  A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it [6].

2. PRINCIPLES OF CRYPTOGRAPHY

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Cryptography is used to achieve the following goals:

- **Confidentiality**

  The data is transmitted at sender side and has to be accessed only by the authorized person and not by anyone else at receiver side.

- **Authentication**

  The data received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or not.

- **Data Integrity**

  Only the authorized person is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

- **Non Repudiation**

  Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

- **Access Control**

  Only the authorized parties are able to access the given information.

3. CLASSIFICATION OF CRYPTOGRAPHY

Cryptography algorithms are classified into two broad categories. They are i) Secret Key Cryptography which is also known as symmetric Key Cryptography ii) Public Key Cryptography which is also known as Asymmetric Key Cryptography.

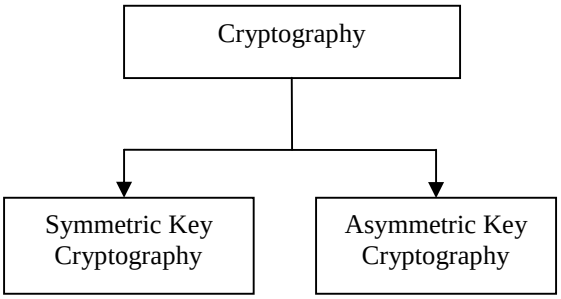

Figure 1 Classification of Cryptography

If the same key is used for encryption and decryption, we call the mechanism as Symmetric Key Cryptography. However, if two different keys are used in a cryptographic mechanism, wherein one key is used for encryption, and another, different key is used for decryption; we call the mechanism as Asymmetric Key Cryptography [2].

Symmetric Key Cryptography

Symmetric Key Cryptography is referred to by various other terms, such as Secret Key Cryptography or Private Key Cryptography. In this scheme, only one key is used and same key is used for both encryption and decryption of messages. Obviously, both the parties must agree upon the key before any transmission begins and nobody else should know about it. As shown in Figure 2, at the sender's end, the key transforms the plain text message into a cipher text form. At the receiver's end, the same key is used to decrypt the encrypted message, thus deriving the original message out of it. With this form of Cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret [6].

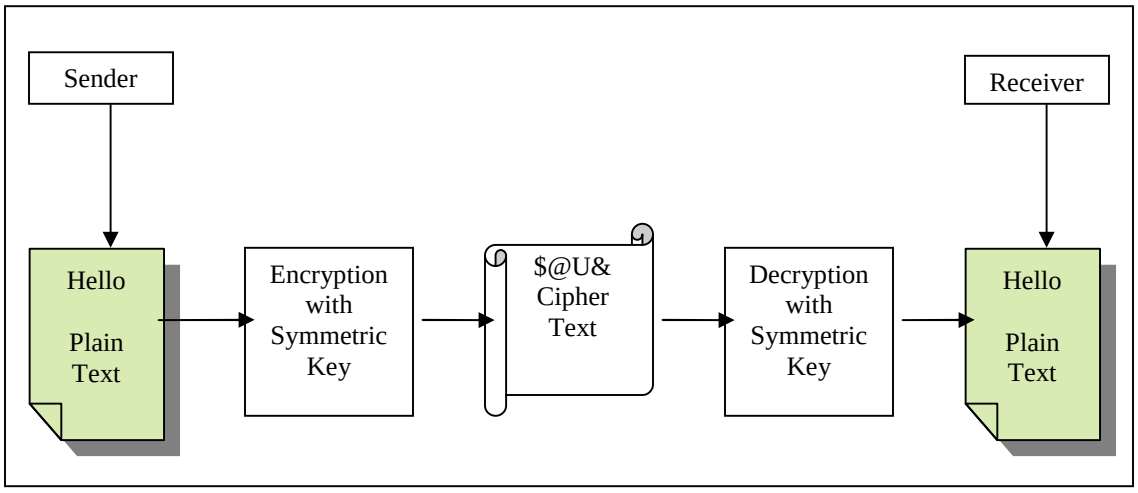

Figure 2 Secret Key Cryptography

Asymmetric Key Cryptography

In Asymmetric key Cryptography, also called as Public Key Cryptography, two different keys (which form a key pair) are used. One is Private Key and other one is public key.

Private Key is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. It is used to decrypt the cipher text encrypted with public key by the sender.

On the other hand, the public key is for the general public. It is disclosed to all parties that you want to Communicate with. In this scheme, in fact, each party or node publishes its public key. Using this, a directory can be constructed where the various parties or nodes (i.e. their ids) and the corresponding public keys are maintained. One can consult this and get the public key for any party that one wishes to communicate. Figure 3 describes the Public Key Cryptography [3].

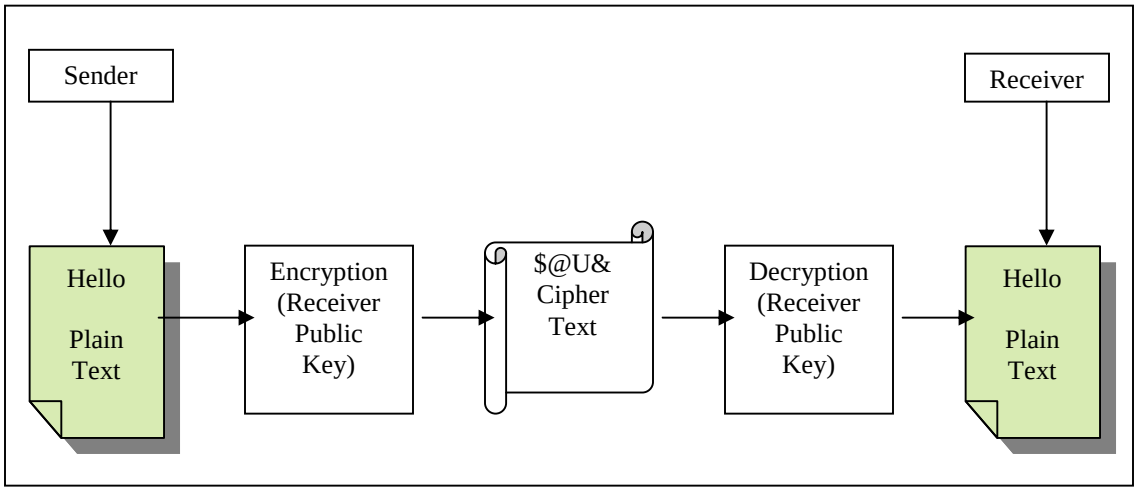

Figure 3 Public Key Cryptography

4. SYMMETRIC KEY CRYPTOGRAPHY

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing.

A block cipher is so called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher [1]. Stream ciphers come in several flavors but two are worth mentioning here. *Self-synchronizing stream ciphers* calculate each bit in the keystream as a function of the previous n bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit keystream it is. Synchronous stream ciphers generate the keystream in a fashion independent of the message stream but by using the same key stream generation function at sender and receiver. While stream ciphers do not periodic so that the keystream will eventually repeat.

Block ciphers can operate in one of several modes; the following four are the most important; Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) mode and Output Feedback (OFB). The most common secret-key cryptography scheme used today is the Data Encryption Standard (DES), designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) in 1977 for commercial and unclassified government applications. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks [4].

There are a number of other secret-key cryptography algorithms that are also in use today like CAST-128(block cipher), RC2 (block cipher), RC4 (stream cipher), RC5 (block cipher), Blowfish (block cipher), Two fish (block cipher). The Advanced Encryption Standard (AES) became the official successor to DES in December 2001.

5. NEW SYMMETRIC KEY ALGORITHM

A Simple symmetric key algorithm is proposed as below

ENCRYPTION ALGORITHM

Step 1: Obtain the order of the letter in alphabetic order.
Step 2: Generate the binary value of the corresponding order. [Binary value should be 8 digits]
Step 3: Take 8 bit binary number as key.
Step 4: Add binary value of letter obtained in step 2 and 8 bit key.
Step 5: Reverse the value obtained in step 4.
Step 6: Subtract the key value from the Reversed number.
Step 7: Obtain its decimal value for the number get from step 6. This would be the encrypted text (cipher text).

DECRYPTION ALGORITHM

Step 1: Obtain the binary form of cipher text.
Step 2: Add key with binary form of cipher text.
Step 3: Reverse the added value.
Step 4: Subtract the key from reversed value.
Step 5: Obtain its decimal form value.
Step 6: Obtain the corresponding letter from alphabetic order for decimal value to get the original text (plain text).

Example

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

Encryption

Step 1: Order of letter "T" in alphabetic is 20.
Step 2: The Binary value of 20 is 10100. Since it is not an 8 bit binary number we need to make it as 8 bit binary number. The 8 bit binary value of 20 is 00010100.

0	0	0	1	0	1	0	0

Step 3: Let 00011001 as 8 bit key.
Step 4: Add binary value of 20, i.e. 00010100 and the key 00011001. The resultant binary value is 00101101.

0	0	1	0	1	1	0	1

Step 5: Reversed value of this resultant binary value is 10110100.

1	0	1	1	0	1	0	0

Step 6: Subtract the key 00011001 from reversed value 10110100. The resultant binary value is 10011011.

1	0	0	1	1	0	1	1

Step 7: The decimal equivalent of binary value 10011011 is 155. The cipher text of this encryption algorithm is 155.

Decryption

After encrypting "T", we have 155 as the cipher text. Now we use the decryption algorithm to get back the original text "T".

Step 1: The 8 bit binary value of cipher text 155 is 10011011.

1	0	0	1	1	0	1	1

Step 2: After adding key with this binary value of cipher text, the result would be 10110100.

1	0	1	1	0	1	0	0

Step 3: After reversing it would be 00101101.

0	0	1	0	1	1	0	1

Step 4: After subtracting key from the reversed value, the result would be 00010100.

0	0	0	1	0	1	0	0

Step 5: The decimal value of 00010100 is 20.In alphabetic order the 20th letter is "T" i.e. the original text.

6. ADVANTAGES OF THE NEW ALGORITHM

1. The Algorithm is very simple and run faster.
2. Reverse and subtract operations in this algorithm makes it more secure.
3. CRC checking in receiving ends is easier.
4. For a small amount of data this algorithm will work very perfectly.

7. CONCLUSION

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication of data. In order to achieve these goals various algorithms are developed by various people. The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms to encrypt a small amount of data. The Symmetric key is run faster than Asymmetric Key and its memory requirement is less our next task would be increasing the key size for this algorithm and also to develop and design a public key cryptographic algorithm in a simple manner as it is done in this paper.

8. REFERENCES

1) S.William, "Cryptography and Network Security: Principles and Practice", 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.

2) Atul Kahate, "Computer and Network Security", 2nd edition, Tata McGraw Hill.

3) Fundamentals of Computer Security, Springer publications "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptolntroLhtm#Algorithms

4) S.Hebert, "A Brief History of Cryptography", an article available at A Simple Symmetric Key Cryptographic Algorithm.doc

5) Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Vol. 1 No. 15, 2010.

6) Monika Agarwal and Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering, Vol. 4 No. 05, pp. 877-882, May 2012.