A Symmetric Key Cryptographic Algorithm

Ayushi
Lecturer, Hindu College of Engineering
H.No:438, sec-12, sonipat, Haryana

ABSTRACT
Any communication in the language that you and I speak—that is the human language, takes the form of plain text or clear text. That is, 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 of achieving security by encoding messages to make them non-readable. **Cryptography** is the practice and study of hiding information. 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 is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

There are two basic types 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, various symmetric key algorithms in detail and then proposes a new symmetric key algorithm. Algorithms for both encryption and decryption are provided here. The advantages of this new algorithm over the others are also explained.

Categories & subject descriptors
[Cryptography & Steganography]: *A New Algorithm*.

General Terms
Algorithms, Design, Security.

Keywords
Cryptography, Network security, Symmetric Key.

1. INTRODUCTION
During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords.

One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. 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*. Cryptology embraces both cryptography and cryptanalysis.

A *cryptographic algorithm*, or *cipher*, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a *key*—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: 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*.
"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.
Usually, the harder it is to discover the key, the more secure the mechanism. In symmetric (also called "secret-key" and, unfortunately, "private key") encryption, the same key (or another key fairly easily computed from the first) 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 and disadvantages.

2. CRYPTOGRAPHY

Data that can be read and understood without any special measures is called plaintext or clear-text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher-text. The process of reverting cipher-text to its original plaintext is called decryption.

In a typical situation where cryptography is used, two parties (X and Y) communicate over an insecure channel. X and Y want to ensure that their communication remains incomprehensible by anyone who might be listening. Furthermore, because X and Y are in remote locations, X must be sure that the information she receives from Y has not been modified by anyone during transmission. In addition, she must be sure that the information really does originate from Y and not someone impersonating Y. Cryptography is used to achieve the following goals:

2.1 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.

2.2 Data integrity

To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication code 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.

2.3 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.

3. TYPES OF CRYPTOGRAPHY

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or cleartext) into ciphertext (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are i) Secret Key Cryptography which is also known as Symmetric Key Cryptography and ii) Public Key Cryptography which is also known as Asymmetric Key Cryptography.

In other words, 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. This is shown in Figure 1 [2]

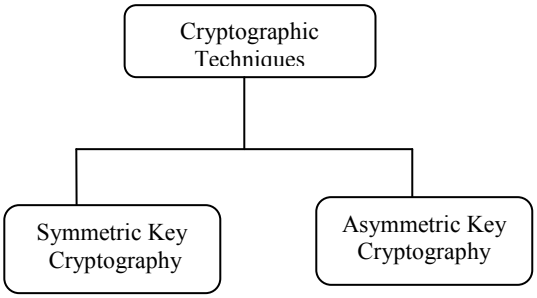

Figure 1 Cryptography techniques

3.1 Secret key cryptography

In secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. 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. The biggest difficulty with this approach, of course, is the distribution of the key [5].

3.2 Public key cryptography

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It 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.

On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. Figure 3 describes the Public Key Cryptography [3].

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.

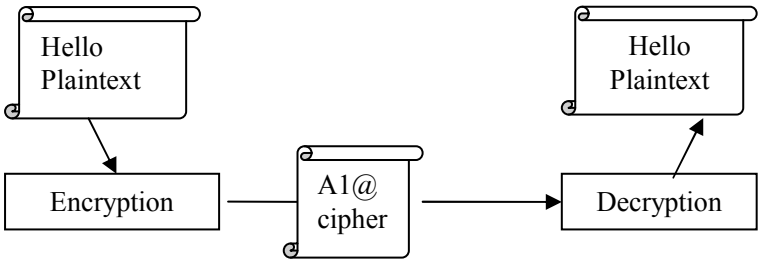

Figure 2 Secret Key Cryptography

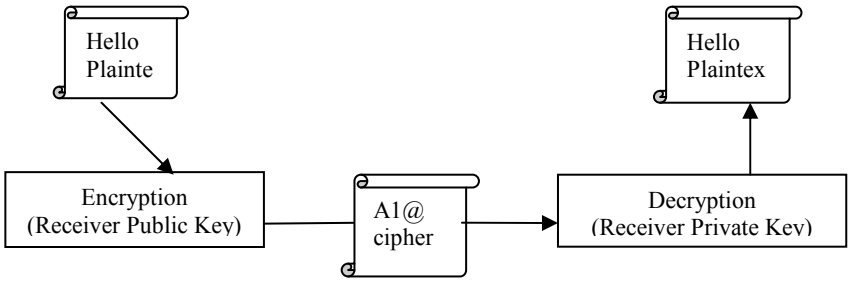

Figure 3 Public Key Cryptography

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 ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext 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 keystream generation function at sender and receiver.
While stream ciphers do not propagate transmission errors, they are, by their nature, 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) [6]. 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) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications. DES has been adopted as Federal Information Processing Standard 46 (FIPS 46- 3) and by the American National Standards Institute as X3.92). 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). In 1997, NIST initiated a process to develop a new secure cryptosystem for U.S. government applications. The result, the Advanced Encryption Standard (AES), became the official successor to DES in December 2001.

5. NEW SYMMETRIC KEY ALGORITHM

5.1 Encryption algorithm

Step 1: Generate the ASCII value of the letter

Step 2: Generate the corresponding binary value of it.

[Binary value should be 8 digits e.g. for decimal 32 binary number should be **00**100000]

Step 3: Reverse the 8 digit's binary number
Step 4: 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 and 5 digits long respectively. If any of these are less then 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the cipertext i.e. encrypted text.
Now store the remainder in first 3 digits & quotient in next 5 digits.

5.2 Example

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

5.3 Decryption algorithm

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 plain text

5.4 Another case study

After encrypting "T" we have got 01000101 as the ciphertext. Now according to decryption algorithm let's try to get back the original text i.e. "T"
Step 1: After multiplying 00101 (last 5 digits of the ciphertext) 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

6. ADVANTAGES OF THE NEW ALGORITHM

1. The Algorithm is very simple in nature
2. There are two reverse operations present in this algorithm which would make it more secured
3. CRC checking in receiving ends is easier
4. For a small amount of data this algorithm will work very smoothly.

7. CONCLUSION

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data
Now, in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. 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 (which are not cost-effective) to encrypt a small amount of data. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues. A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm. But as public key cryptography is more secured then secret key cryptography our next task would be 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) Computer and Network security by ATUL KAHATE

3) 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

4) S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

5) "Introduction to Public-Key Cryptography", an article available at
developer.netscape.com/docs/manuals/security/pkin/contents.htm