A Symmetric Key Encryption Algorithm

Saiesh N. Prabhu Verlekar
Department of Information technology
SRIEIT, Shiroda, Ponda, Goa, India

Abstract- Computer encryption is based on the science of cryptography, which has been used as long as humans have wanted to keep information secret. In order to protect sensitive data and distribution we rely on using cryptographic schemes, such as certificates or encryption keys. Thus, cryptography mechanisms form a foundation upon which many important aspects of a solid security system are built. Most forms of cryptography in use these days rely on computers, simply because a human-based code is too easy for a computer to crack. Ciphers are also better known today as algorithms, which are the guides for encryption as they provide a way in which to craft a message and give a certain range of possible combinations. A key, on the other hand, helps a person or computer figure out the one possibility on a given occasion. Before the digital age, the biggest users of cryptography were governments, particularly for military purposes.

Cryptography is the art of achieving security by encoding messages to make them non-readable. It is the practice and study of hiding information. 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. This paper describes cryptography, types of cryptography and then proposes a new Symmetric key algorithm.

Keywords – Cryptography, Symmetric Key, Asymmetric Key.

I. INTRODUCTION

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. [1]

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 which may be a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different cipher text 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. [1] 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. We will refer to a message that is readable, or not encrypted, as plaintext, clear text and denote it with the symbol M. The process of disguising a message to hide its substance is called encryption. We will represent this operation as E (M). The encrypted message, C=E (M) is called cipher text. The process of turning cipher text back into plaintext, M=D(C), is called decryption. Cryptography is the art and science of keeping messages secure.

In addition to providing confidentiality, cryptography is also used for:

a) Authentication: receiver can determine the origin of the message and an intruder cannot masquerade.

b) Integrity: receiver should be able to verify that the message has not been modified in transit. An intruder cannot substitute a false message for the original.

c) No repudiation: a sender should not be able to falsely deny that he sent a message.

d) Confidentiality: a message may be encrypted so that others cannot read its contents.

A cryptographic algorithm, or cipher, is the mathematical function used for encryption/decryption. If the security of an algorithm is based on keeping it secret, it is a restricted cipher. Restricted ciphers are historically interesting but

not adequate today. With a changing user community, everything is lost if the wrong party discovers the cipher. Moreover, there is no ability to have quality control on the algorithm since it must be kept hidden. Far more preferable are ciphers that rely on a publicly-known algorithm that accepts a secret parameter, or key, for encryption and decryption. If the encryption and decryption keys are the same, the algorithm is known as a symmetric algorithm.

$$C = E_K (M)$$
$$M = D_K (C)$$

If the key used for encryption is different from the key used for decryption, then the algorithm is a public-key algorithm The decryption key cannot be calculated from the encryption key in a reasonable amount of time (and vice versa). The reason it is called a public-key algorithm is because the encryption key can be made public. A stranger can thus encrypt a message with this public key but only the holder of the decryption key (private key) can decrypt the message. A message can also be encrypted with the private key and decrypted with the public key. This is used as a basis for digital signatures. Anyone can decrypt the message with the public key but by doing so; they know that only the possessor of the private key was able to encrypt it. [3]

II. THE PURPOSE OF CRYPTOGRAPHY

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:

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]

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. [2]

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. [2]

III. TYPES OF CRYPTOGRAPHY

Cryptography is a process which is associated with Scrambling plaintext (ordinary text, or clear text) into cipher text (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. [1] 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.

IV. SYMMETRIC CRYPTOGRAPHY

In symmetric or secret key cryptography, a single key is used for both encryption and decryption. the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver as shown in fig. 1.

The receiver applies the same key (or rule set) 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.

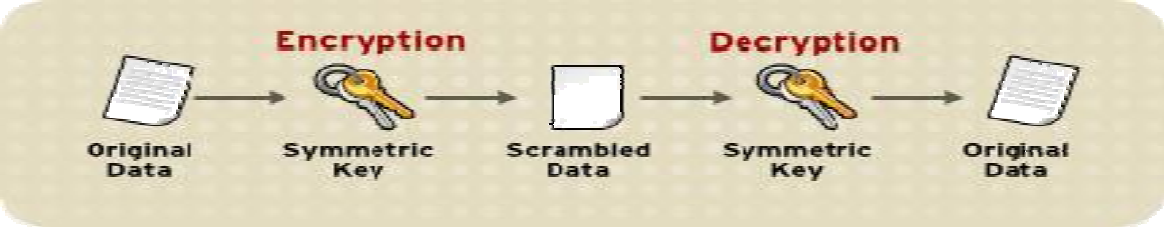

Fig.1 Symmetric-Key Encryption

V. ASYMMETRIC KEY CRYPTOGRAPHY

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key as shown in fig. 2. 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.

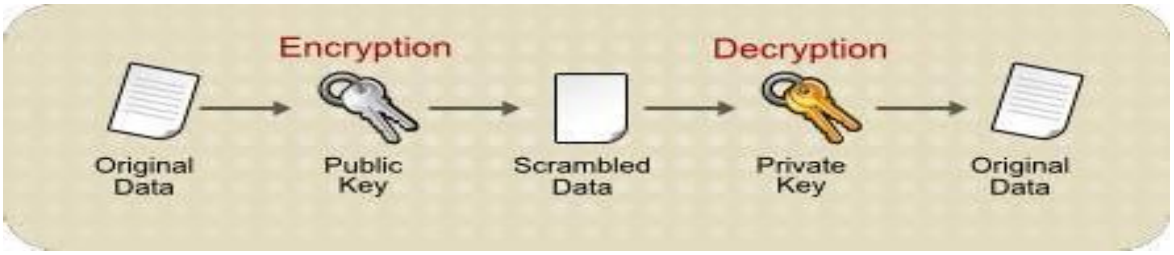

Fig.2 Asymmetric-Key Encryption

VI. SYMMETRIC KEY ALGORITHM

6.1. 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 (no matter how much the length of it, we should represent it in 8 digits (2^8=256).

Step 3: Reverse the 8 digit's binary number.

Step 4: Take a 16 bit Key.

Step 5: Divide the reversed number with the divisor.

Step 6: Store the remainder in first 3 digits & quotient in next 5 digits. 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 cipher text i.e. encrypted text.

6.2 Decryption Algorithm

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

Step 2: Add first 3 digits of the cipher text 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.

VII.CONCLUSION

It has been found that the algorithms which are available at this moment are more or less difficult or complex in nature because those algorithms are used to maintain high level of security against any kind of forgeries.

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 encrypt a small amount of data with 16 bit key. More the key size, more stronger the algorithm. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner.

REFERENCES

[1] "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.htmlAlgorithms
[2] K. Gary, *"An Overview of Cryptography"*, an article available at www.garykessler.net/library/crypto.html
[3] Lectures on Cryptographic communication and authentication by Paul Krzyzanowski.
[4] A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount by Mohammad Zakir Hossain Sarker and Md. Shafiul Parvez.
[5] A Symmetric Key Cryptographic Algorithm by Ayushi.
[6] Symmetric Key Management Systems by Arshad Noor.
[7] Practical Symmetric Key Cryptography on Modern Graphics Hardware by Owen Harrison and John Waldron.
[8] On Hiding Message Length in Symmetric-key Cryptography by Cihangir Tezcan.