ISSN 2278-3091
Volume 6, No.2, March - April 2017
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse03622017.pdf

A Proposed Method for Cryptography using Random Key and Rotation of Text

Mousumi Ghanti[1] Prof. Samir Kumar Bandyopadhyay[2]
[1] Student, Department of Computer Science and Engineering, University of Calcutta
2 Professor, Department of Computer Science and Engineering, University of Calcutta

ABSTRACT

Cryptography is an emerging technology and important for network security. The widespread use of computerised data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorised access while in storage or transmission. The only general approach to sending and storing data over media which are insecure is to us some form of encryption. A primary concern is that many attacks involve secret manner access to information resources, and organizations are often unaware of unauthorized access to their information systems. In this paper symmetric key encryption method is used for security purpose.

Keywords: Information security, Encryption, Decryption, Cryptography

1. INTRODUCTION

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the cipher text. There are two types of cryptography—1.Symmetric –key cryptography and 2.Asymmetric –key cryptography. . There are various types of algorithm of cryptography like AES, DES, RSA, Caesar etc.

Though different approaches are there for securing data still nobody can strongly ensure that with those algorithms the data are safe now. Each and every day people are proposing new techniques in this field. Here in my approach, I have used Symmetric –key cryptography where the key value is generated randomly and this key is used to encrypt the data and as well as decrypt. After generating the key value, the data bits are shifted with k bit rotation (K is random value). This is shown in figure 1.

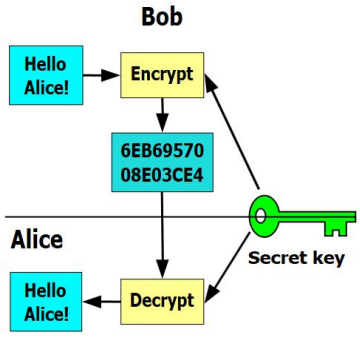

Figure 1 Generation of Secret Key

The only general approach to sending and storing data over media which are insecure is to use some form of encryption. A primary concern is that many attacks involve secret manner access to information resources, and organizations are often unaware of unauthorized access to their information systems. A Symmetric encryption algorithms are extremely effective at transforming a lot of data and computationally less intensive than asymmetric encryption algorithms. There are two sorts of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively.

2. REVIEW WORKS

"Cryptography" derives from the Greek word kruptos, meaning "hidden" [1]. 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 [2]. Cryptography, the science of encrypting and decrypting information, dates as far back as 1900 BC when a scribe in Egypt first used a derivation of the standard hieroglyphics of the day to communicate [3] .There are many notable personalities who participated in the evolution 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:

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 [4]. For ensuring 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 [4]. 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 [4].

Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extensions to the check summing techniques that we encountered in reliable transport and data link protocols. Cryptography is an emerging technology, which is important for network security. The widespread use of computerised data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorised access while in storage or transmission. Due to continuing advancements in communications and eavesdropping technologies, business organisations and private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques, which, until very recently, were exclusively used by the military and diplomatic communities. Cryptography is a vital of today's computer and communications networks, protecting everything from business e-mail to bank transactions and internet shopping While classical and modern cryptography employ various mathematical techniques to avoid eavesdroppers from learning the contents of encrypted messages. Computer systems and networks which are storing, processing and communicating sensitive or valuable information require protection against such unauthorised access [5-6].

3. PROPOSED METHODOLOGY FOR ENCRYPTION AND DECRYPTION

The symmetric encryption approach is divided in to two types one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography but here block cipher type is used because its efficiency and security is good as compared to other. Proposed technique uses a common key between sender and receiver, which is known as private key. Basically private key concept is the symmetric key concept, where plain text is converted into encrypted text known as cipher text using private key and cipher text is decrypted by same private key into plain text. The method is described below.

1) Read the plaintext from a text file. E.g
StreamReader reader = new StreamReader("C:/crypto/mousumi.txt");

2) Read the text character by character and rotate right (k bit rotation) to encrypt.

For rotation--

- ch1 = (char)(byte)(((byte)ch << k) | ((byte)ch >> (8 - k)));
  Here variable **k** is holding the random generated key value.

3) Now store the encrypted text in another file. E.g.

```
using (StreamWriter sw = File.AppendText("C:/crypto/mou.txt"))
        {
          sw.Write(ch1);
        }
```

4) Again read the encrypted text from the predefined file . E.g.

```
StreamReader reader1 = new StreamReader("C:/crypto/mou.txt");
```

5) Read the text character by character and rotate left (k bit rotation) to encrypt.
For rotation—

- ch1 = (char)(byte)(((byte)ch >> k) | ((byte)ch << (8 - k)));

6) Now store the decrypted text in another file.

3.1 STEPS OF RANDOM KEY GENERATION

For random key generation, two variable low and high for ensuring limit are used. With help of constructor and random function the key value is generated and stored in another variable so that same random value can be used for encryption and decryption.

```
Random rand;
int high, low, v;
public Rotation()
{
    this.rand = new Random();
    this.high = 7;
    this.low = 1;
    this.v = (rand.Next() % (high + 1 - low)) + low;
}
```

3.2 STEPS OF ROTATION

```
class Rotation
  {
    Random rand;
    int high, low, v;
    public Rotation()
    {
      this.rand = new Random();
      this.high = 7;
      this.low = 1;
      this.v = (rand.Next() % (high + 1 - low)) + low;
    }
    public char rightrot(char ch)
    {
      char ch1;
      int k = v;
      ch1 = (char)(byte)(((byte)ch << k) | ((byte)ch >> (8 - k)));
      return ch1;
    }
    public char leftrot(char ch)
    {
      char ch1;
      int k = v;
      ch1 = (char)(byte)(((byte)ch >> k) | ((byte)ch << (8 - k)));
      return ch1;
    }
  }
```

The proposed method has the following advantages:

- Reduce Time complexity.
- More Flexibility.
- Better Security.
- More Reliance on users.
- Binary string (for fast access)

4. CAESAR CIPHER ENCRYPTION TECHNIQUE

Caesar cipher is an example of substitution method. Caesar decided that shifting each letter three places down the alphabet in the message would be his standard algorithm, and so he informed all of his generals of his decision, and was then able to send them secured messages. The method is implemented below.

Algorithm

```
int main () {


char cipher[50];

int shift;


  printf("Enter text to be encrypted IN CAPITAL LETTERS ONLY: ");

  scanf("%s", cipher);


  printf("How many shifts do you prefer? 1-10 only: ");

  scanf("%d", &shift);


  caesar (cipher, shift);


  return 0;

}


void caesar (char cipher[], int shift) {

  int i = 0;


  while (cipher[i] != \0') {

   if ((cipher[i] += shift) >= 65 && (cipher[i] += shift) <= 90) {

     cipher[i] += (shift);

   } else {

     cipher[i] += (shift - 25);

   }

   i++;

  }

  printf("%s", cipher);

}
```

In the above algorithm to encrypt a text proposed algorithm requires Text and encryption key. The encryption key is an integer value and it determines alphabet to be used for substitution. It is based on modulo twenty six arithmetic to ensure that integer value wraps round in case encryption key supplied is more than twenty six. Decryption follows reverse operations per Formed during the process of encryption. It requires decryption key, and encrypted text. The decryption key should be complement to the encryption key so that reverse character substitution can be achieved. As stated earlier, Caesar cipher simply shifts encrypted character by number of positions. In this paper we can use three methods, where key size isfixed. First method is depend on the address of message, second depend on the length of first word in message and third method is depend on number of words in first line. Furthermore, the characters of the encrypted text are scrambled in such a way that if an attempt is made to decrypt the cipher text it would not be easy to decrypt the text.

The main difference between the above two techniques are—

- In Caesar cipher key value is static
- In our implementation key value is generated dynamically.
- Static value is more likely to be hacked by malicious users. But it is quite tough to guess the random generated (dynamic) key value. And therefore I can say that our applied technique is more secured than Caesar technique.

5. CONCLUSIONS

The symmetric key process is simple enough and both of the trading partner can use same encryption algorithm and same secret key. They do not need to bother about different key values. Moreover, generally the keys for symmetric key ciphers are relatively short.

REFERENCES

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

[2] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[3] Betty Huang. Analysis of the RSA Encryption Algorithm, Computer System Lab 2009-2010.

[4] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh. Comparative Study of DES, AES and RSA,

[5] J.A. Bondy and U.S.R Murty,"Graph Theory with Application", Macmillan Press Ltd, First Edition 1976.

[6] Betty Huang. Analysis of the RSA Encryption Algorithm, Computer System Lab 2009-2010