Volume 2 No. 4, April 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

http://www.esjournals.org

RDA Algortihm: Symmetric Key Algorithm

Dinesh Goyal,Vishal Srivastava
Arya College of Engineering & Technology, Kukas, Jaipur

ABSTRACT

Cryptography is an art of illusion in which the sender encodes the message using a key and sends it over the communication channel. The receiver on the other side of the channel decodes the message back and using the key tries to obtain back the original message. If the key during the communication is same on both sides then it is called as symmetric key cryptography and if is called as asymmetric key cryptography. There has been different encoding techniques used for the pain text in both block & stream cipher mode some of them are ECB & CBC for block cipher & OFB & CBC for block cipher.
Vigenere Cipher is a Caesar Cipher substitution technique where in a Caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D,B would become E and so on . The Vigenere cipher consists of several Caesar ciphers in sequence with different shift values. To encipher, a table of alphabets can be used, termed a Vigenere square, or Vigenere table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword. Decryption is performed by finding the position of the cipher text letter in a row of the table, and then taking the label of the column in which it appears as the plaintext. For example, in row L, the cipher text .L appears in column A, which taken as the first plaintext letter. The second letter is decrypted by looking up x in row E of the table; it appears in column T, which is taken as the plaintext letter.
In this paper an attempt is made to design a new model of Symmetric key Cryptography using Vigenere Cipher Technique and ECB Encoding.

Keywords: *RDA Algorithm, symmetric key*

1. INTRODUCTION

Cryptography means the study of secret (crypto) writing (graphy). It can be defined as the science of using mathematics to encrypt and decrypt data back [1]. It allows two people to communicate with each other securely. This means that an eavesdropper will not be able to listen in on their communication. Cryptography also enables the receiver to check that the message sent by the sender was not modified by the interceptor and that the message he receives was really sent by sender [2].

A message is known as a plaintext or clear text. The method of disguising the plaintext in such a way as to hide its information is encryption and the encrypted text is also known as a cipher text. The process of reverting cipher text is shown in figure 1.1[3].

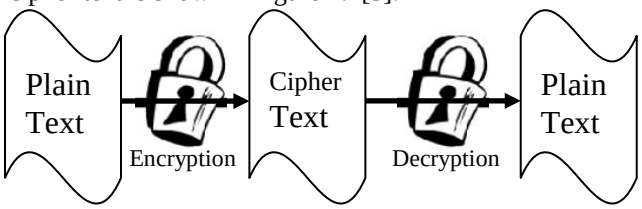

Figure 1.1 Cryptography for secure communication

There have been many techniques which have evolved over the period of time for encrypting and decrypting of the text which can be basically techniques.

Substitution ciphers encrypt plaintext by changing the plaintext one piece at a time.

Plaintext	V	O	Y	A	G	E	R
Key	+3	+3	+3	+3	+3	+3	+3
Cipher text	Y	R	B	D	J	H	U

There have been many kind of substitution techniques evolved till now few of them are:

1. Caesar Cipher
2. mono alphabetic Cipher
3. Homophonic Cipher
4. PolyGram Cipher

On the other hand transposition cipher encrypts plaintext by moving small pieces of the message around. Anagrams are a primitive transposition cipher.

V	O	Y	A	G	E	R
O	V	A	Y	E	G	R

There have also been many techniques used for transposition, few of which are:

1. Rail Fence Technique
2. columnar Transposition
3. Vernam Cipher
4. Book Cipher

Symmetric key algorithms have used two modes of encryption & decryption namely Stream & Block cipher.

Stream cipher encrypts plaintext one byte or one bit at a time. A stream cipher can be thought of as whereas Block cipher with a really small block size, whereas block ciphers encrypt plaintext in chunks. Common block sizes are 64 and 128 bits.

Different modes of encoding have been used in block cipher which are:

Electronic codebook (ECB)

The simplest of the encryption modes is the electronic codebook (ECB) mode. The message is divided into blocks and each block is encrypted separately.

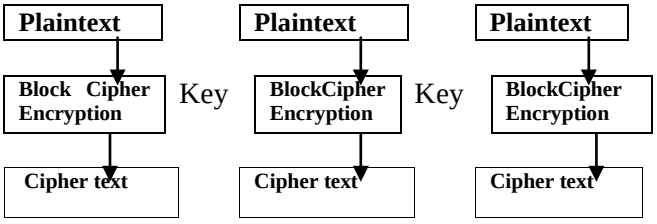

Fig 1.2 ECB Encryption Encoding (Source wikipedia. org)

1.2 Cipher- block chaining (CBC)

CBC mode of operation was invented by IBM in 1976. in the cipher-block chaining (CBC) mode, each block of plaintext block before being encrypted. This way, each cipher text block is dependent on all plainest blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the fist block.

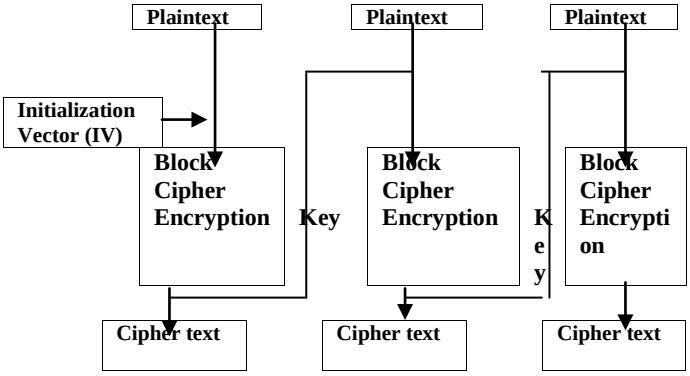

Fig 1.3 CBC Encryption Encoding(SOURCE wikipedia. org)

Output feedback & Cipher feedback are the two stream cipher encoding techniques.

2. VIGENERE CIPHER MODEL

The ignore cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. it is a simple form of polyalphabetic substitution technique.

This cipher is well known because while it is easy to understand and implement, it often appears to beginners to be unbreakable; this earned it the description le chuffer indecipherable (French for 'the unbreakable cipher'). Consequently, many people have tried to implement encryption schemes that are essentially ignore ciphers, only to have them broken.

2.1 History of Vignere Cipher

The first well documented description of a polyalphabetic cipher was formulated by Leon Battista Alberta around 1467 and used a metal cipher disc to switch between cipher alphabets. Alberta's system only switched alphabet after several words, and switched were indicated by writing the letter of the corresponding alphabet in the chiphertxt.later, in 1508,Johannes trithemius,in his work poligraphia,invented the tabula recta,a critical component of the ignore cipher. Trithemius, however, only provided a progressive, rigid and predictable system for switching between cipher alphabets.

The ignore cipher has been reinvented many time. The method was originally described by Giovan Battista Bellaso in his 1553 book La cifra del.Sig.Giovan Battista Bellaso;.He built upon the tabula recta of trithemius, but added a repeating "countersign" (a key)to

switch cipher alphabets every letter,however,the scheme was later misattributed to Blaise de Vigenere in the 19th century, and is now widely known as the "Vigenere cipher".

Blaise de Vigenere published his description of a similar but stronger auto key cipher before the court of Henry III of France, in 1586.Later, in the 19th century; the invention of Bellaso's cipher was misattributed to Vigenere. David Kahn in his book The code breakers lamented the misattribution by saying that history had "ignored this important contribution and instead named a regressive and elementary cipher for him [Vigenere]though he had nothing to do with it".

2.2 Description

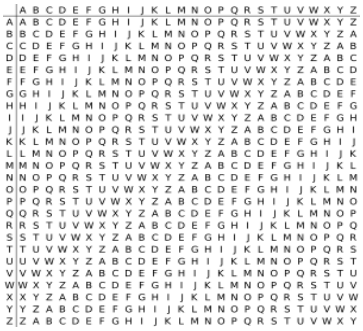

Fig 1.4 the Vigenere square or Vigenere table, also known as the tabula recta, can be used for encryption and decryption.

In a Caesar cipher, each letter of the alphabet is shifting along some number of places; for example, in a Caesar cipher of shift3, A would become D, B would become E And so on. The Vigenere cipher consists of several Caesar cipher in sequence with different shift values.

To encipher, a table of alphabets can used, termed a *tabula reacta*, *Vigenere square*,or *Vigenere table*.it consists of the alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers At different point in the encryption process,the cipher uses a different alphabet from one of the rows.the alphabet used at each point depends on a repeating keyword.

For example, suppose that the plaintext to be encrypted is:
ATTACKATDAWN

The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword
"LEMON"

LEMONLEMONLE

The first letter of the plaintext, A, is enciphered using the alphabet in row L, which is the first letter of the key. This is done by looking at the letter in row L and column A of the Ignore square, namely L.similary, for the second letter of the key is used; the letter at row E and column T is X. the rest of the plaintext is enciphered in a similar fashion:

Plaintext: *ATTACKATDAWN*

Key: *LEMONLEMONLE*

Cipher text: *LXFOPVEFRNHR*

Decryption is performed by finding the position of the cipher text letter in a row of table, and then taking the label of the column it which it appears as the plaintext. For example, in row L, the chipertext L appears in column A, which takes as the first plaintext letter. The second letter is decryption by looking up x in row E of the table; it appears in column T, which is taken as the plaintext letter.

Vigenere can also be viewed algebraiacally.if the letter A-Z are taken to the numbers 0-25,and addition is performed modulo 26, than Vigenere encryption can be written as:

$$Ci = Pi + Ki \pmod{26}$$

And decryption,

$$Pi = Ci + Ki \pmod{26}$$

3. PROPOSED MODEL

A new model is here by proposed by combing the Vigenere cipher model and ECB encoding model where instead of using a static key pattern (used in original Vigenere cipher model) we are using a dynamic key pattern by shifting the key matrix n number of times for m rounds.

In this new model the plain text is modified into the cipher text by adding some value in each round and then the obtained value is added 32X 32(1024) times with different key values. After every round of 1024

modification key pattern is changed by matrix is generated using the Vigenere table technique.

In the proposed model the encryption work is performed by:

CI =(PI +KI)mod 256

And decryption is performed

PI=(CI-KI)mod 256

This model gives birth to a symmetric key algorithm and is not easily available for crackoing. The proposed algorithm works for 1024 bytes of data and can be extended into multiple folds of 1024 byts for a big size of data.

4. PROPOSED ALGORITHM

4.1 Algorithm for Encryption

```
void encrypt_ file ()
{
  int  x =0,j=0,k;

//Open file for matrix conversion

FILE *file = fopen (file_ name, "r");
If (file = =0
{
   puts("\n\Na file error occurred. File does not exit. \n");
getch();
exit (1);
}

//filling plain text array with file content

while( x    <= 1023 && ( plaintext_ array
[x]=getc (file))!=EOF)
       {
              x++;
        }
Plaintext _ array [x]='\0';

//creating matrix 32 of plain text array

x=0;
for(i=0;j<32&&plaintext_array[x]!='0';i++)
      {
for (i=0;i<32&& plaint_ array [x]!='0;j++)
                {
                    pt [i][j]=plaintext_array[x];
                 }
        }
 pt[i][j]='0';

//to close file after matrix conversion

fclose (file);

//to generate the key 2d array

fill_key_ array();

//process of encryption performed in four rounds

for(k+0;k<4;k++)
{
for(i=0;i<32;i++)
          {
             for(j=0;j<32;j++)
               {
        ea[i][j]=(pt[i][j]+ka[i][j]%256;
                  }
             }
//method called to shift the key matrix
      shift_any();
    }

//file opened for encryption in write mode

file=fopen(file_name, "w");
if(file = = 0)
 {
puts ("A file error occurred. File  does not exist.");
exit(1);
}
x =0;

//process of writing the encrypted code back into the
file

for(i=;i<32&plaintext_arrayx]!='\0';++)
{
for(i=;i<32&plaintext_arrayx]!='\0';++)
      {
       fprintf (file, "%c", ea[i][j];        x++);
        }

//file closed after writing
 fclose (file);
}
```

4.2 Algorithm for Decryption

```
void decrypt_file()
{
       int x=0,I,j,k;

// encrypted file opened in read mode to copy it into a
array

FILE *file  = fopen  (file_name, "r");
If (file)== 0)
{
        puts ("\n\nA file error occurred. File does not exist.
\n");
exit(1);

// file copied in a ID array

while (x<= 1023 && (encrypted_array
[x]=getc(file))!=EOF)
          {
              x++;
}
necrypted_array[x]='\0';

// converting the data into 2D array

  for(i=0;i<32 && encrypted _array[x]!='\0';j++)
{
  for(j=0;j<32 && encrypted _array[x]!='\0';j++)
    {
                  ea[i][j]=encryoted_array[x];
                 x++;
         }
     }

// file closed for the moment

fclose (file);
file_key_array();

// process of generating the plain text back from cipher
text

for(k=0;k<4;k++)
 {
   for(i=0;i<32;i++)
    {
      for(j=0;j<32;j++)
        {
            pt[i][j]=(ea[i][j]- ka[i][j]) % 256;
        }
      }

    // shifting the key array

     shift_ary();
}

// file opened for writing back the plain text into

             file = fopen (file_name, "w");
              if (file = =o-0)
              {
puts ("\n\A file error occurred.  File does not exist. \n");
exit (1);
              }
             x=0;
              i=0;
              j=0;

// writing plain text into file

for(i=0;i<32 && encrypted_array{x}!='\0'i++)
 {
  for(j=0;j<32   && encrypted_array[x]!='\0';j++)
         {
           fprintf   (file, "%c" pt[i][j])
             x++;             }
      }
      fclose (file);
}
```

4.3 Method For Shifting The Key Array During The Process Of Encryption& Decryption So That Every Time New Key Is Used:

```
void shift_ary()
{
char ay[32][32];

// intermediate array

int i=0,j=0;

// process for generating the shift key array

              for(i=0;i<32;i++)
               {
                      for(j=0;j<32;j++)
                     {
                             ay[i][j]=ka[(i+N)%32][j];
```

```
                }
}
```

// process for storing the shifted key array

```
        for(i=0;i<32;i++)
            {
                for(i=0;j<32;j++)
                 {
                        ka[i][j]=ay[i][j];
                 }
             }
}
```

4.3 Method for Filling the Key Array during the Process of Encryption & Decryption:

```
void fill_key_array()
{Int I,j=0;
Printf ("\n\n enters the word (max 1023, min 1). \n");
Gets ( key _array);
For (i=0;<1024;i++)//calculating length of key
 if (key _array[i]=='\0')
break;
while(i<1024)//filling key array
{
        key_ array [i]=key _ array [j];
        j++;
        j++;
}
```

//creating matrix of key array

```
      for (i=0;<32;i++)\
        {
            for (j=0;j<32;j++)
              {
                    ka [i] [j] =key _array [x];
                    x++;
               }
           }
   }
```

5. CONLCUSION

This paper gives short introduction to the world of Cryptography. I have shown all the simplest methods of Cryptography work and how they can be explored. I have discussed the methods of encoding and the concept of block and stream cipher.

Further in this paper the Vigenere Cipher model has been explored right from its history to its methodology of working and thus tries to find the draw backs in the same.

Next it poses a new model of public key symmetric key cryptography using ECB encoding techniques for a caeser cipher like model called vigenere cipher model designed for secure message transcription between two users.

The algorithm has been designed and executed and tested and also provides authentication.

The complexity in this paper can further be extended by using either by using CBC encoding technique and increasing the number of rounds and improving the complexity of the key.

ACKNOWLEDGMENTS

We would like to thank Dr. Shiv Kumar, Professor, Arya College of Engineering & Technology, Jaipur for his esteemed guidance.

REFRENCES

[1] David Kahn, The Code breakers, 1967 ISBN 0-684-831330-0.

[2] Oded Goldreich, Foundations of cryptography, volume 1: Basic Tools,Cambridge university press, 2001, ISBN 0-521-7917-3

[3] Cryptolog (Definition)'. Merriam-webster's Collegiate Dictionary (11th editioned.). Merriam-Webster.com http://www.merriam-Webster.com/ dictionary /cryptology/. Retrieved on 2008-02-01

[4] http://www.wikipedia.org

[5] Singh, Simon (1999). "Chapter 2:Le Chiffre Indechiffrable". The code book. Anchor Book Random House. Pp.63-78 ISBN 0-385-49532-3.