ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(4): 115-117
www.allresearchjournal.com
Received: 19-02-2017
Accepted: 20-03-2017

Mousumi Ghanti
Student of Computer Science and Engineering. University of Calcutta, Kolkata, West Bengal, India

Samir Kumar Bandyopadhyay
Department of Computer Science and Engineering University of Calcutta, Kolkata, West Bengal, India

Correspondence
Mousumi Ghanti
Student of Computer Science and Engineering. University of Calcutta, Kolkata, West Bengal, India

A method for encryption of secret message

Mousumi Ghanti and Samir Kumar Bandyopadhyay

Abstract
For secure transmission over network cryptography was used. The algorithm selected for cryptography should fulfil the conditions of integrity protection, conventional message authentication and digital signatures. Here in our paper we have studied present algorithms currently used for encryption.

Keywords: Public key algorithm, symmetric key algorithm, hash function, cipher text, key length

Introduction
Cryptography is the practice of secure data communication in the presence of third party. Cryptography encrypt the data at the transmitter end to protect it from stolen and from errors. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. It deals with mathematics, computer science and electrical engineering. Cryptography comes from the Greek words for "secret writing." It has a long and colorful history going back thousands of years. Professionals make a distinction between ciphers and codes. A cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. In contrast, a code replaces one word with another word or symbol. Codes are not used any more, although they have a glorious history [1-2]. The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the cipher text, is then transmitted, often by messenger or radio.

Review Works
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 [3]. Stream ciphers are of many types but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the key stream as a function of the previous n bits in the key stream. It is termed "selfsynchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit key stream it is. One problem is error propagation; a garbled bit in transmission will result in n garbled bits at the receiving side. Synchronous stream ciphers generate the key stream 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 propagate transmission errors, they are, by their nature, periodic so that the key stream will eventually repeat. Block ciphers can operate in one of several modes; the following four are the most important: • Electronic Codebook (ECB) mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a cipher text block. Two identical plaintext blocks, then, will always generate the same cipher text block. Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others.

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well [4-5].

Algorithm for Cryptography:

```
#include<stdio.h>
#include<conio.h>
#include<string.h>
int main()
{int l,n,j,i=0,count,flag,t;
char
str[100],temp,str1[100],str2[5],str3[]="AC100",str4[5],str5[]
="12345",str10[100];
printf("\n\tenter any string: ");
gets (str);
l=strlen(str);
printf ("\n\tASCII value of each character of given string: ");
While (str[i])
printf(" %d ",str[i++]);
j=i-1;
i=0;
while(i<j)
{temp=str[i];
str[i]=str[j];
str[j]=temp;
i++;
j--;}
printf("\n\tresult after revarsal\t\n");
for(i=0;i<l;i++)
{printf("%d\t",str[i]);}
for(i=0;i<l;i+=2)
{temp=str[i];
str[i]=str[i+1];
str[i+1]=temp;}
printf("\n\nafter swapping--\n");
for(i=0;i<l;i++)
printf("%d\n",str[i]);
printf("\n\tthe text after adding key--\n");
for(i=0;i<l;i++)
{str1[i]=str[i]+5;
printf(" %d ",str1[i]);}
printf("\n\t--the final encrypted text is--\n\t");
for(i=0;i<l;i++)
{printf("%c",str1[i]);}
printf("\n\t Do you want to decrypt the above text??
\n\t1.YES\n\t2.NO--");
scanf("%d",&n);
if(n==1)
{printf("\n\tenter your ID : ");
scanf("%s",&str2);
if(strcmp(str2,str3)==0){
count=1;
printf("\n\t Congratulations!!\t Your ID is matched..!!\n\t
Enter your Password: ");
scanf("%s",&str4);
while(strcmp(str4,str5)!=0 && count<3)
{printf("\n\t Wrong Password!!..Try Again..Remember You
will be blocked after 3 attempts..");
scanf("%s",&str4);
count++;
flag=1;}
if(strcmp(str4,str5)==0)
{printf("\n\t Congratulations!!\t Your PASSWORD is
matched..!");
t=1;}}}
else if(n==2)
printf("\n\t Thank you..!! Have a nice Day..");
if(t==1)
{printf("\n\tthe text after subtracting key--\n");
for(i=0;i<l;i++){
str10[i]=str1[i]-5;
printf(" %d ",str10[i]);}
for(i=0;i<l;i+=2)
{temp=str10[i];
str10[i]=str10[i+1];
str10[i+1]=temp;}
printf("\n\nafter swapping--\n");
for(i=0;i<l;i++)
printf("%d\n",str10[i]);}
printf("\n\tresult after revarsal\t\n");
for(i=l-1;i>=0;i--)
{printf("%d\t",str10[i]);}
printf("\n\tyour decrypted text is here--\n");
for(i=l-1;i>=0;i--)
printf("%c",str10[i]);
return 0;}
```

Results

```
enter any string: i love india
ASCII value of each character of given string: 105 32 108
111 118
101 32 105 110 100 105 97
result after revarsal
97 105 100 110 105 32 101 118 111 108 32 105

after swapping--
105
97
110
100
32
105
118
101
108
111
105
32

the text after adding key--
110 102 115 105 37 110 123 106 113 116 110 37

--the final encrypted text is--
nfsi%n{jqtn%
Do you want to decrypt the above text??
1.YES
2.NO--1

enter your ID : AC100
Congratulations!! Your ID is matched..!!
Enter your Password: 12456

Wrong Password!!..Try Again..Remember You will be
blocked after 3 attem
pts..12345
```

```
Congratulations!! Your PASSWORD is matched..!
the text after subtracting key--
105 97 110 100 32 105 118 101 108 111 105 32

after swapping--
97
105
100
110
105
32
101
118
111
108
32
105

Result after revarsal
105 32 108 111 118 101 32 105 110 100
105 97

Your decrypted text is here--
i love india
--------------------------------
Process exited after 25.14 seconds with return value 0
Press any key to continue.
```

Conclusions: Cryptography has been emerged as essential tool for data transmission. Various algorithms of cryptography has been studied, If advantages of all these algorithms are combined in one algorithm then performance of cryptography can be increased along with the length of key. In public key algorithm for generation of private key

References

1. Rogaway P, Shrimpton T. Cryptographic Hash Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance‖ FSE, 2004.
2. Jim Alves-Foss,‖ An E_cient Secure Authenticated Group Key Exchange Algorithm for Large and Dynamic Groups.
3. Black J, Rogaway P, Shrimpton T. Black-box analysis of the block-cipher-based hash function constructions from PGV. In Advances in Cryptology – CRYPTO ’02, volume of Lecture Notes in Computer Science. Springer-Verlag, 2002, 2442.
4. Mao W. Modern Cryptography: Theory & Practice. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference, 2004.
5. Vishwa gupta, Gajendra Singh, Ravindra Gupta. Advance cryptography algorithm for improving data security‖ IJARCSSE. 2012; 2:1.