Modified One Time Pad Data Security Scheme: Random Key Generation Approach

Sharad Patil sd_patil057@rediffmail.com

Research Student,
Bharti Vidyapeeth,
Pune, India

Manoj Devare deore.manoj@gmail.com

Vidya Pratishthan's
Institute of Information Technology,
Baramati(MS), India

Ajay Kumar ajay19_61@rediffmail.com
Jaywant institute ,
Pune(MS), India

ABSTRACT

In this articles we show how the random key stream can be used to create lifetime supply of keys for one time pads. Here we provided the practical approach that you can use to set up your own one-time pad encryption. For simplicity let's study how randomized key can be achieved. Random key generation can simply be obtained via use of permutation. Permutation techniques can be used in conjunction with other technique includes substitution, encryption function etc. for effective performance. The goal of this article to show how the one-time pad encryption technique can be achieved by a combining of these techniques.

Keywords :- Cryptography, Cryptosystem, One-time pad, encryption, auto-key , Key enhancement, Digital Signature.

1. INTRODUCTION

Today's networks are seriously threatened by network attacks. Besides the rapid improvement of attacking technologies powered by profits, there are three reasons that cause the present serious status of network security, including internet itself having a weak basis, the current security technologies having respective drawbacks and limitations and the dilemma between security performance and according cost. By considering this three , in this article , we try to put secure one time pad scheme with random key generation approach.

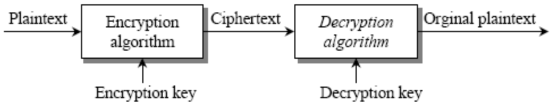
One well known realization of perfect secrecy is the One-time Pad, which was first decscibed by Gillbert Vernam in 1917 for use in automatic encryption and decryption of telegraph messages. It is interesting that the One-time Pad was thought for many years to be an " unbreakable" cryptosystem, but there was no mathematical proof of this until shannon developed the concept of perfect secrecy over 30 year later.

1.1 Cryptosystem for One time Pad : Let n ≥1 be an interger and take Þ =e = k = (Z2)n .
For K ε (Z2)n , define eK (x) to be the vector sum modulo 2 of K and x (or equivalently , the exclusive –or of the two associated bitstrings) So, If x=(x1….xn) and K=(K1…..Kn) then
eK (x)= (x1 +K1….. ,xn + Kn) mod 2
Decryption is identical to encryption.
If y=(y1….yn) , then , dK (y)= (y1 +K1….. ,yn + Kn) mod 2 [3]
Vernam patented his idea in the hope that it would have widespread commeracial use . but due to unconditionally secure cryptosystem like one time pad , the amount of key that must be communicated securely is at least as large as the amount of plaintext. The one-time pad is vulnerable to a known-plaintext attack. If the key is used once for every plaintext , it creates the severe key management

From the experimet it is easily seen that the One-time Pad provides perfect secrecy and not breakable becacuse of the two facts , encryption key is random number and the key is used once only. The system is also more attractive because of easily encryption and decryption. One time pad has been empolyed where unconditional security may be of great importance includes military and diplomatic context.

It should be clear that the one-time pad is discarded after a one time use, so this technique is highly secure and suitable for small message only and impractical for large message.

1.2 Cryptography



Cryptography may be used at different levels of a security model. The algorithms used, the quality of their software implementation and the key length used are the main factors determining the strength of a cryptography application.

Cryptography can reformat and transform your data, making it suffer on its trip between computers. The technology is based on the essentials of secret codes arguments by modern mathematics and protects your data in powerful ways

Secret code= Encryption – digital Signature

1.3 Biometric security

For many organizations, implementing the right biometric user identification technique can improve data security and lead to significant cost savings by reducing help desk calls Biometric user authentication techniques can be used to protect PCs and networks from unauthorized access by authenticating users based on a physical feature such as a fingerprint, retina, iris, hand, or face. Although voice and signature identification do not involve physical characteristics, they are usually included with biometric user authentication techniques. For some of these biometric techniques, the cost of the equipment needed to identify a user is too high for widespread use. For example, the cameras and equipment needed for iris scanning can cost thousands of dollars. However, iris scanning is one of the most accurate biometric user authentication techniques, and it is expected to be used extensively in applications such as user identification for automatic teller machines (ATMs).

2. PRELIMINARIES

Basically there are two type of random number generators used in cryptography, the true random number generator[TRNG] and the pseudorandom number generators[PRNG]. The aim of a TRNG is to generate individual bits, with uniform probability and without any correlation between those bits. Consequently , the knowledge of some bits does not give any information about the other generated bits. However , achieving this task in real practice appears to be a difficult possibility . Consequently the cryptographic designers and implementers often do resort to pseudorandom bit generators in many applications. [3]

A long random [or pseudo –random] string used to encrypt a message with a simple EX-OR operation is known as a one tine pad. A stream cipher generates a one time pad and applies it to a stream of plaintext with EX-OR.

2.1 History

A little bit history of cryptography as a science or art , was originally developed by the Arabs. The year 1412 saw the publication of Subh-al-a “sha, a, a 14-volume encyclopedia written by shihab al-Din. The text explain transposition and substitution.

The one-time pad system itself was perfected in 1917 during the first World war. Random keys were written on paper that were glued together to form the pad. In this encryption technique the key used once hence refer as one-time pad. An army Signal Corp. officer, Joseph Mauborgne , proposed an improvement to Vernam cipher that give concrete ultimate in security. A long random[or pseudo random] string used to encrypt a message with a simple Ex-OR operation known as a one-time-pad. The key stream for a one-time pad must be a true random stream, mean that every key byte can take any value in between 1 to 256 octets. The practical difficulty of this encryption scheme is that the key bytes cannot be used again.

Law PAD1: The one-time pad is a method of key transmission, not message transmission. [Blakeley] . The One-Time Pad is just a simple variation on the Beale Cipher.

2.2 One time pad system

The one-time pad encryption scheme is define as any method of encryption where each byte of the plaintext is encrypted using one byte of the key stream and each key byte is used once only. Hence name as One time pad.

One time pad encryption algorithm can be known from the following equation
C i = E(P i ,K i) for I= 1,2,3,……n
Where : E = the encryption parameter
P I= the ith character of the plaintext
Ki = the ith bytes of the key used for massage
C i =the ith character of the cipher text
n = length of the key stream.
Both the encryption parameter and Key stream must be kept secret .

For practical application , the key used for one time pad cipher is a string of random bits, usually generated by a Cryptographically Strong Pseudo-Random Number Generator. However for ultimate security , it is suggested to generate the key by using the natural randomness of quantum mechanical events, since quantum events are believed scientifically to be the only source of truly random information in the universe.

If the key is truly random an XOR operation based one –time pad encryption scheme is perfectly secure against cipher text-only cryptanalysis.

We come to the point that if the hackers does not know the sender or receiver key, then the one time pad encryption scheme is 100 % secure. We can only talk about OTP if four important rules are followed. If these rules are applied correctly, the one-time pad can be proven to be unbreakable (see Claude Shannon's "Communication Theory of Secrecy Systems"). However, if only one of these rules is disregarded, the cipher is no longer unbreakable.

1. The key is as long as the plaintext.
2. The key is truly random (not generated by simple computer Rnd functions or whatever!)
3. There should only be two copies of the key: one for the sender and one for the receiver (some exceptions exist for multiple receivers)
4. The keys are used only once, and both sender and receiver must destroy their key after use.

In Short One Time pad has the characteristics

* if a truly random key as long as the message is used, the cipher will be secure
• called a One-Time pad
• is unbreakable since cipher text bears no
statistical relationship to the plaintext

• since for **any plaintext & any cipher text**
there exists a key mapping one to other
• can only use the key once though
• have problem of safe distribution of key

2.3 Advantages and disadvantage of one time pad

Message encrypted by using One Time Pad cannot be broken because of, the fact that , encryption key is a random number and the key is used only once. However the practical difficult of using One-Time Pad is that the key bytes cannot be reused.

What we are doing to enhance the security ?

Today, more than ever, computer networks are utilized for sharing services and resources. Information traveling across a shared IP-based network, such as the Internet, could be exposed to many devious acts such as eavesdropping, forgery and manipulation. Fortunately, there are several mechanisms that can protect any information that needs to be sent over a network. This paper introduces One Time pad security mechanism and explains available security mechanisms to effectively prevent such threats from happening.

No one wants his or her confidential or classified information revealed. Confidential information that you do not want to share with others is the easiest to protect, but ever so often there is a need to share this type of information. Whenever this happens, you need to be able to send the information in a secure manner to your trusted receiver. This issue is particularly important when network communication is involved, since network communication has become the cornerstone for organizational effectiveness and today’s digital communication often includes sensitive information such as control and corporate financial data. Consequently, we need security mechanisms whenever sensitive information is to be exchanged over the network. And hence it need tobe improve the security upto optimize level.

3. METHODOLOGY

We used simulation methodology to check the encrypted text for alphabets. Here we first create the ASCII chart for small alphabet that shown in Table-1 and then generate the random number key after that enter the plain text which we want to sent to the recipient as most secure one, then next access the equivalent ASCII number of given plain text from Table-1 hereafter we add the first ASCII character equivalent number and the first random key number i.e. we add key to the plain text. then implement the equivalent ASCII character of addition repeat the process still end of string , then write the encrypted text. While sending the encrypted text to the recipient we must add the random number key at the end of encrypted text , key factor is that here at the begin of encrypted message we add the first number that treat as the length of plain text which can be helpful for the recipient to identify the actual string or message.

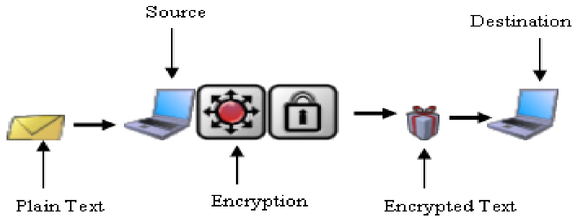


Fig.1-Encryption Process by Random Key generation (At source)

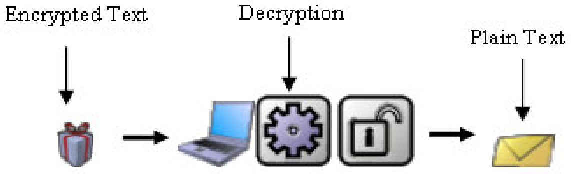


Fig.2-Decryption Process at destination

Here the practical information is used that can be used to setup one time pad encryption system. For easy adoption the steps is given 1] create the key 2] format the massage 3] Encrypt the massage 4] Decrypt the massage . The Figure 1 and Figure 2 shows the easiest map for the process. The proposed method of encryption is shown in Figure -1 . This process is done at source host. The part of decryption process will be performed at the destination end. that shown in Figure -2

4. ALGORITHM

```
* Random Key Generation ( );
Step-1 Create Ascii Chart ( ) ;
Step-2 Create random_array();
Setp-3 Create Get_Plain_Text( )
Step 4 Write _file for Plain text()
Step 5 Create encrypted Text ()
Step 6 Write file for encrypted text()
Step 7 Send the encrypted file to the recipient
Step 8 Perform decryption process
Step 9 get the Plain text at the destination
Step 10 end
```

Table-1 Sample Ascii chart

Alphabet	ASCII	Alphabet	ASCII
a	97	n	110
b	98	o	111
c	99	p	112

d	100	q	113
e	101	r	114
f	102	s	115
g	103	t	116
h	104	u	117
i	105	v	118
j	106	w	119
k	107	x	120
l	108	y	121
m	109	z	122

5. IMPLEMENTATION AND ANALYSIS AND RESULTS

```
#include <stdlib.h>
#include <stdio.h>
FILE *fp;
int cntr,i,var,index;
int len,other;
int random_array[10];
char plain_text[10];
char encrypt_text[20];
char decrypt_text[20];
char alphabet[26];
int ascii[26];
void get_plain_text();
void create_ascii_chart();
void create_random_array();
void write_file();
void create_encrypt_text();
void create_decrypt_text();

void main()
{
clrscr();
randomize();
alphabet[0]='a';
create_ascii_chart();
create_random_array();
get_plain_text();
write_file("p.txt",plain_text);
create_encrypt_text();
write_file("e.txt",encrypt_text);
create_decrypt_text();
write_file("d.txt",decrypt_text);
//Decide whether to ADD/substract/multiply/divide by
//available random values to the original text/table
getch();
}


void write_file(char *file_name,char *str)
{
        fp=fopen(file_name,"w");
        fputs(str,fp);
        fclose(fp);
}
```

```
void create_ascii_chart()
{
        printf("Contents of alphabet Array\n");
        for(cntr=0;cntr<26;cntr++)
        {
                alphabet[cntr]=alphabet[0]+cntr;
                ascii[cntr]=alphabet[cntr];
                printf("%c\t%d\n",alphabet[cntr],ascii[cntr]);
        }

}

void create_random_array()
{
        printf("The ten random numbers are=\n");
        for(i=0;i<=10;i++)
        {
        random_array[i]=rand()%10;
        printf("number is[%d] =%d\n",i,random_array[i]);
        }
}

void create_encrypt_text()
{
var=0;
index=0;
other=0;
len=strlen(plain_text);
for(index=0;index<len;index++)
{
        for(other=0;other<26;other++)
        {
                if(plain_text[index]==alphabet[other])
                {
                encrypt_text[index]=ascii[other]+random_array[index];
                break;
                }
        }
}
//append radom_array/KEY to the encrypted format
for(i=0;i<10;i++)
{
encrypt_text[index]=random_array[i];
index++;
}
printf("\n\nEncrypted Text=");
printf("%s",encrypt_text);
}
void get_plain_text()
{
printf("\nPlease enter plain Text.[no space, max. 10 character] .\n");
        gets(plain_text);
        printf("Your Plain text is=");
        puts(plain_text);
}
void create_decrypt_text()
{
```

```
var=0;
index=0;
other=0;
len=strlen(encrypt_text);
for(index=0;index<len;index++)
{
        for(other=0;other<26;other++)
        {
                if(encrypt_text[index]==alphabet[other])
                {
                decrypt_text[index]=ascii[other]-random_array[index];
                break;
                }
        }
}
//append radom_array/KEY to the encrypted format
for(i=0;i<10;i++)
{
decrypt_text[index]=random_array[i];
index++;
}
printf("\n\nDecrypted [Plain text] Text=");
printf("%s",decrypt_text);
}
```

In this type of encryption system ,we took only small lower case alphabets and their ASCII value , so by using ASCII code of the alphabets and random generated key , the encrypted text is more complex and it's analysis is difficult for attackers. Hence I come to conclusion that by designing different encryption method as a onetime pad is more difficult for crack. In further research ,we would like to design the algorithm on modular arithmetic base with complements concepts.

6. CONCLUSION & FUTURE WORK :

This algorithm has a lot of scope to enhance the security by using combining the different approaches such as binary addition, multiplication and modular arithmetic function are also common. instead of using ASCII . We have outlined a number of defense strategies, many of which demand much further research. The algorithm become more dynamic if we choose the above approaches randomly. In further research we would like to design the algorithm on modular arithmetic base with complements concepts.

7. REFERENCES

1. Larry l. Peterson et al. "Computer Networks –A Sysytem Approach ", Third Edition , Morgan Kaufmann Publishers ISBN:0-55860-833- 8.

2. Behrouz A. Forouzan et al., " Data Communication and Networking " Third Edition , TATA McGRAW –HILL EDITION ISBN-0-07-058408- 7.

3. Douglas R, Stinson " CRYPTOGRPHY Theory and Practice " Second Edition .

4. Charlie Kaufman st al. " Network Security " PRIVATE Communication in a PUBLIC World. , Prentice Hall of India Private Limited. 2003

5. Information Technology Journal 4(3) : 204-221, 2005

6. Claude Shannon's " Communication Theory of Secrecy Systems" .
7. Neal R. Wagner "The Laws of Cryptography: Perfect Cryptography: The One-Time Pad "
8. Ritter, Terry 1991. The Efficient Generation of Cryptographic Confusion Sequences. Cryptologia "15: 81-139.
9. www.EFYMAG.com - February-2007

10. www.zdnetindia.com

11 .www.sans.org