Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Advanced & Secure Authentication System through Enhanced OTPs

Chandaka Babi, Alvala Naresh
Department of Information Technology
GIT, Gitam University, Vizag
Andhra Pradesh, India

Abstract—Cryptography is an art and science of converting original message into non-readable form means 'secret writing'. Two techniques are used for converting data into non-readable form: 1) Transposition technique 2) Substitution technique. One Time Pad is an example of substitution method. As One Time Pad has various limitations so this talk will present an enhanced one time pad technique perspective on combination of techniques substitution and transposition. A double columnar transposition method is applied on One Time Pad in order to overcome limitations of One time Pad cipher and provide much more secure and strong cipher. This paper however proposes a hypothesis regarding the use of enhanced one time pad based protocol and is a comprehensive study on the subject of using enhanced one time pad technique. This forms the basis for a secure communication between the communicating entities.

Key words—One Time Pad (OTP), Random, Attacks Security Threats, cryptography, One Time Pad cipher, Cryptographic Techniques and Information Security.

I. INTRODUCTION

In this modern age people use networks and communication facilities for transmission of data between them. So Network Security measures are needed to protect data during transmission.

For Network Security came the concept of **Cryptography** meaning is "Secret Writing" is the most effective and strongest tool for controlling against many types of security attacks. A well designed data cannot be modified, read or fabricated. So **Encryption** is the process to change data in a form that cannot be get easily.

Encryption is an effective way to achieve the security of data. The word of encryption came in mind of King Julius Ceaser because he did not believe on his messenger so he thought to encrypt the data or message by replacing every alphabet of data by 3rd next alphabet. The process of Encryption hides the data in a way that an attacker cannot hack the data. The Simple data is known as Plain text and Data after encryption is known as **Ciphertext**.

In cryptography, onetimepad (OTP) is an encryption technique. OTP, also called **Vernam-Cipher** or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key. A one-time pad is a cryptosystem invented by vernam. It's a very simple system and is unbreakable if used correctly. In this technique, a plaintext is paired with a random secret key (or pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition.

II. USING AN OTP

One time pads are used in pairs. The more copies of a given pad, the greater the likelihood is that one may be captured, in which case the system is completely broken. One copy of the pad is kept by each user, and pads must be exchanged via a secure channel e.g.: face to face on floppy disks. The pad is used by XORing every bit of the pad with every bit of the original message. Once the message is encoded with the pad, the pad is destroyed and the encoded message is sent. On the recipient's side, the encoded message is XORed with the duplicate copy of the pad and the plaintext message is generated.

One-time pad encipherment can be denoted as:

Ci = E (Pi, Ki)

Where E is the enciphering operation, Pi is the i-th character of the plaintext, Ki is the i-th byte of the key used for this particular message, and Ci is the i-th character of the resulting cipher text. Both the key stream K and the enciphering operation E are secret. The key for each individual message is the starting location in the entire random key stream used for this encipherment.

For efficiency, it is good practice to start each message near the position following the key byte used for the last character of the previous message. This eliminates the need to keep track of which portions have been used, and removes the danger that a message will be longer than any of the remaining segments.

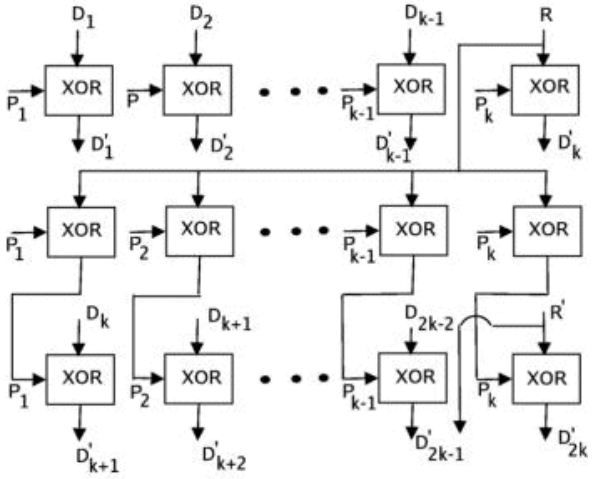

Figure.1 Cryptographic techniques for one time pad

2.1 Working Of OTP:

Basically sender has the random OTP, which both sender and intended recipient have. Sender has a message M, and he computes the cipher text C by XORing the message with the OTP:

C = M xor OTP

Sender sends the cipher text to his recipient, the recipient knowing the OTP also can recover the message by computing the reverse, XORing the cipher text C with the OTP:

M = C xor OTP

Sender must never re-use the OTP, otherwise it wouldn't be a "One-Time" pad anymore, and it would lose it's unbreakable properties as information would start to be leaked.

2.2 OTP in different languages

OTP in 1 line of perl:

```
vec($_,0,1);open(P,shift);read(P,$p,length),print  $_^$pwhile<>
```

OTP in 1 line of C:

```
main(i,c)int*c;{for(c=fopen(c[1],"r");i=~getchar();putchar(getc(c)^~i));}
```

Applications:

1. The onetimepad is the most optimal cryptosystem with theoretically perfect secrecy.
2. The onetimepad can be used in super-encryption.
3. The algorithm most commonly associated with quantum key distribution is the onetime pad.
4. The onetimepad is mimicked by stream ciphers.
5. The onetimepad can be a part of an introduction to cryptography.

Disadvantages:

1: The key is as long as the message and it too must be transmitted securely to the recipient before the message can be sent.

2: No integrity protection

3: Keys cannot be reused

III. ENHANCEDONETIMEPAD

Army Signal Corp. Officer, Joseph Mauborgne, proposed an improvement to Vernam Cipher that was the ultimate in security. He suggested that we use a random key that is as long as the message means the key need not to be repeated. In additional key must be use once for encryption and decryption of a single message and then that key is discarded. So this technique is called as One Time Pad and there is relationship between key and plaintext and it is unbreakable. In this as advance of vignere cipher scheme we Can use 27 character in which 27th character is SPACE, so in this key will be as long as message. So table of Vignere cipher must be expanded to 27*27.

PT	A	B	C	D	E	F	G	H	I
CT	0	1	2	3	4	5	6	7	8
PT	J	K	L	M	N	O	P	Q	R
CT	9	10	11	12	13	14	15	16	17
PT	S	T	U	V	W	X	Y	Z	‘Space’
CT	18	19	20	21	22	23	24	25	26

1. The encryption and decryption algorithm is known.
2. Only 2 keys are to try.

3. The language of the plaintext is known and easily recognizable.
4. Need of absolute synchronization between sender and receiver.
5. Need for an unlimited numbers of keys.
6. Generating a large number of random keys is no problem but printing, distributing, storing and accounting for such keys are problems.

3.1 ALGORITHM:

There is an algorithm which is used to encrypt and decrypt the data which enhance the more security of One Time Pad cipher than original One Time Pad.

A. Encryption Algorithm:-

1) We take a message or plaintext from user which we have to encrypt.
2) Then decide the key1, using which we get the characters after finding out the values in One Time Pad 27th characters tableau.
3) Encrypt the message by replacing each letter using decided key1.
4) Now write the encrypted message or output of the step3 in rectangle way, row by row. The number of rows depends on the amount of data.
5) Now the order of column becomes the key2 to this algorithm, which is decided by sender for encryption and also known by receiver.
6) Read off the message column by column.
7) Output of step 6 is again written in rectangle form, as above done.
8) After placing the data so, we again read it column by column and we get out our result.
9) Finally we get the secure cipher text (Encrypted data) to forward securely.

B. Decryption Algorithm:-

An algorithm used in reverse order to get the plaintext is known as decryption algorithm.
1) It takes cipher text, key1, key2 as input which is also known by receiver.
2) Arrange the cipher text in rectangle form: column by column using order of key2.
3) Now read off the data row by row.
4) Repeat the step 2 and 3 using output of step 3 as input.
5) Now decrypt the output of step 4 with key1: using one time pad tableau.
6) Finally we get the original message.

Example:

Encryption:

1) Suppose the original message is **THIS IS A TEXT**.
2) Suppose the key1 is FJPWOMAEISDBKZ.
3) Encrypt the data using key1 and the cipher text is: YQXNNUSDIRWFGR
4) Suppose the key2 is 2 3 1 4 which is number of column and also specify their order. It can be anything according to the sender.
5) Now arrange the output of step 3 in rectangle format

Key: **2 3 1 4**
Plaintext: Y Q X N
N U S D
I R W F
G R

6) Read column by column according to the order and the cipher text is: XSWYNIGQURRNDF.
7) Now write the above cipher in rectangle form

Key: **2 3 1 4**
Plaintext: X S W Y
N I G Q
U R R N
D F

8) Read the data column wise again. The cipher is: WGRXNUDSIRFYQN.
9) Finally we get our secure output.

Decryption:

1) Arrange the cipher in rectangle form: column by column, receiver knows the key2 and number of rows.
First apply k2 on it-

Key: **2 3 1 4**
Plaintext: X S W Y
N I G Q
U R R N
D F

2) Read row by row: XSWYNIGQURRNDF.
3) Again arrange the output in rectangle form column by column:

Key: **2 3 1 4**
Plaintext: Y Q X N
N U S D
I R W F
G R

4) Read row wise, the data is: YQXNNUSDIRWFGR.
5) Using key1 and tableau again we get the same data. **THIS IS A TEXT**.
6) This is original message which is sent by sender.

Applications:
This One Time Pad which is enhanced using Double Columnar Transposition Technique has various advantages over simple One Time Pad technique-
1. There is no chance to cryptanalyze.
2. Result is not easy to reconstruct.
3. Also overcome the limitation of simple One Time Pad.

Disadvantage:
1. Use of Double Transposition technique makes it a complex method.
2. Also difficult to implement.

IV. CONCLUSION

In this paper we have proposed a new methodology through which one time pads can be more secure. One Time Pad is already a strongest Substitution technique and used for high security data. It is a substitution technique in which only letter replaced by any other letter. Transposition techniques are mainly used with other technique to improve the level of security. Only use of Substitution technique replaces the letter by any other letter and only use of Transposition technique changes the place of letters but use of both techniques simultaneously improve the level of security and provide more secure data. The above described method is the combination of both substitution and transposition techniques and provides much more secure data than only use of single Substitution technique.

REFERENCES

[1] Charles P.Pfleeger “Security in Computing”, 4th edition, Pearson Education[1]
[2] William Stallings (2003), *Cryptography and Network Security*, 3rd edition, Pearson Education[2]
[3] http://en.wikipedia.org/wiki/Cryptography[3]
[4] http://en.wikipedia.org/wiki/Onetimepad[4]
[5] C.E. Shannon, “Communication theory of secrecy systems”,Bell System tech. J., 28:657-715, 1949[5]
[6] C. M. Chen, and W. C. Ku, “Stolen-verifier Attack on twoNew Strong-password Authentication Protocol,” IEICETransactions on Communications, Vol. E85-B, No. 11, pp.2519—2521, November 2002.[6]
[7] Id Quantique White Paper, Version 2.0, 2004.[7]
[8] Frank Rubin. One-Time Pad Cryptography, Published in Cryptologia, 20(4): 359 – 364, 1997 [8].

