IMPLEMENTATION OF MULTIPLICATIVE SUBSTITUTION CIPHER WITH KEYED TRANSPOSITION CIPHER FOR ENHANCING NETWORK SECURITY

PRATEEK SRIVASTAVA, BRAMAH HAZELA, SHISHIR SHUKLA

Abstract: In today's world when hacking, data robbery and theft are common phenomena, it is very important to protect data and information that is sent over a particular network. And that is where the need of cryptography arises. Cryptography is an art and science of converting original message into non readable form. There are two techniques for converting data into non readable form: 1) Transposition technique and 2) Substitution technique. When Multiplicative substitution cipher and Keyed transposition cipher techniques are used individually, cipher text obtained is easy to crack. Combining Multiplicative substitution cipher with Keyed transposition cipher can eliminate their fundamental weakness and produce a cipher text that is hard to crack.

Keywords: Cipher Text, Cryptanalysis, Cryptography, Keyed Cipher, Multiplicative Cipher, Substitution, Transposition.

Introduction: The requirements of information security within an organization have undergone major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. Network security measures are needed to protect data during their transmission.

Cryptography [3], a word with Greek origin, means "secret writing". However we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

As cryptography is the science and art of creating secret codes, cryptanalysis [4] is the science and art of breaking those codes. In addition to studying cryptography techniques, we also need to study cryptanalysis techniques. That is needed, not to break other people's codes, but to learn how vulnerable our cryptosystem is.The study of cryptanalysis help us in creating better secret codes.

Types of Cryptography:

There are two main types of cryptography:-

1. Symmetric Key Encipherment
2. Asymmetric Key Enciphermen

Symmetric Key Encipherment (sometimes called secret key encipherment or secret key cryptography) [1] . With this type of cryptography both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Asymmetric Key Encipherment (sometimes called public key encipherment or public key cryptography) [1].It uses a pair of keys for encryption and decryption. With public key cryptography keys work in pairs of matched public and private keys.

Theory of Approaches Used :

Multiplicative Substitution Ciphers :

A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with other. In a multiplicative cipher, the encryption algorithm specifies multiplication of the plaintext by the key and the decryption algorithm specifies division of the cipher text by the key. The plaintext and cipher text are integers in Z_{26} and the key is an integer in Z_{26}*.

In case of Encryption the desired cipher text value would be obtained by (Equation 1):

$$C=(P*K) \bmod 26 \quad (1)$$

where C stands for cipher text value, P stands for original plaintext value and K is the key value chosen by the original sender of the message.

In the case of decryption, the desired plaintext value would be obtained by (Equation 2) :

$$P=(C*K^{1}) \bmod 26 \quad (2)$$

where P stands for plaintext value, C stands for cipher text value and K^{-1} is the inverse of the key being used in the encryption process[1][2]. There is a relation between K and K^{-1} which is obtained by (Equation 3):

$$(K*K^{-1}) \bmod 26=1 \quad (3)$$

This implies that if we have taken the value of K as 3, then the value of K^{-1} would be 9 [1][2]. If we have taken the value of K as 5, then the value of K^{-1} would be 21. The key instances that we choose must belong to the following set S={1,3,5,7,9,11,15,17,19,21,23,25} and the value of K^{-1}will also belong to the above set only.

Keyed Transposition Cipher: A Transposition cipher does does not substitute one symbol for another, instead it changes the location of the symbols. In other words, a transposition cipher reorders (transposes) the symbols.

In Keyed Transposition cipher, encryption or decryption is done in the three steps.

Step 1:- The text is written into a table row by row.

Step 2:- The permutation is done by reordering the columns, according to the assumed key.

Step 3:- The new table is read column by column.

Proposed Work: In the proposed method we will combine multiplicative substitution cipher with keyed transposition cipher to promote user privacy.

Encryption Algorithm:

Step 1:- Take the plaintext as input and encrypt it by using the multiplicative substitution cipher technique.

Step 2:- Pass the cipher text values to keyed transposition cipher technique, where they will be arranged in a row-wise manner.

Step 3:- Assume a key for the encryption and decryption process.

Step 4:- Replace the columns, according to the assumed key.

Step 5:- Read the data in the column-wise manner.

Decryption Algorithm

Step 1:- Read the data row-wise and arrange it column-wise.

Step 2:- Use the assumed key for the decryption process.

Step 3:- Replace the columns according to the assumed key.

Step 4:- Arrange the values in a row-wise manner.

Step 5:- Use the cipher text values and the inverse of key to get the required plain text.

Implementation :

Encryption Process: In case of encryption, the desired cipher text value would be obtained by **(Equation 1).**

Step 1:- Suppose we want to implement these two algorithms for the original message "**INDIA IS A GREAT COUNTRY**". For this purpose we are using the length of key K=5.

PLAINTEXT(P)	ENCRYPTION(E)	CIPHERTEXT(C)
I->08	(8*5)MOD 26	14->O
N->13	(13*5)MOD26	13->N
D->03	(3*5)MOD 26	15->P
I->08	(8*5)MOD 26	14->O
A->00	(0*5)MOD 26	00->A
I->08	(8*5)MOD 26	14->O
S->18	(18*5)MOD 26	12->M
A->00	(0*5)MOD 26	00->A
G->06	(6*5)MOD 26	04->E
R->17	(17*5)MOD 26	07->H
E->04	(4*5)MOD 26	20->U
A->00	(0*5)MOD 26	00->A
T->19	(19*5)MOD 26	17->R
C->02	(2*5)MOD 26	10->K
O->14	(14*5)MOD 26	18->S
U->20	(20*5)MOD 26	22->W
N->13	(13*5)MOD 26	13->N
T->19	(19*5)MOD 26	17->R
R->17	(17*5)MOD 26	07->H
Y->24	(24*5)MOD 26	16->Q

Step 2:- Now these cipher text values will be passed on to the keyed transposition approach, where first of all they will be arranged in a row wise manner as shown below:

O	N	P	O	A
O	M	A	E	H
U	A	R	K	S
W	N	R	H	Q

Step 3:- In this example, we are using the following key for encryption and decryption.

1	3	2	4	5
2	4	3	5	1

Step 4:- The first column would be replaced by second column, the third column would be replaced by fourth column and so on.

N	P	O	A	O
M	A	E	H	O
A	R	K	S	U
N	R	H	Q	W

Step 5:- In the final step, we will read them in column by column manner as shown below:

N	M	A	N	P	A	R	R	O	E
K	H	A	H	S	Q	O	O	U	W

Decryption Process

Step 1:- Read the data row wise and arrange it in the column wise manner.

N	P	O	A	O
M	A	E	H	O
A	R	K	S	U
N	R	H	Q	W

Step 2:- Use the assumed key for the decryption process.

1	3	2	4	5
2	4	3	5	1

Step 3:- The first column would be replaced by fifth column the fifth column would be replaced by fourth column and so on.

O	N	P	O	A
O	M	A	E	H
U	A	R	K	S
W	N	R	H	Q

Step 4:- Arrange the values in a row wise manner

O	N	P	O	A	O	M	A	E	H
U	A	R	K	S	W	N	R	H	Q

Step 5:- We will get the plaintext by **(Equation 2).** In our case the value of K^{-1} will be 21 as the value of K we used was 5.

CIPHERTEXT(C)	DECRYPTION(D)	PLAINTEXT(P)
O->14	(14*21)MOD 26	08->I
N->13	(13*21)MOD26	13->N
P->15	(15*21)MOD 26	03->D
O->14	(14*21)MOD 26	08->I
A->00	(0*21)MOD 26	00->A
O->14	(14*21)MOD 26	08->I
M->12	(12*21)MOD 26	18->S
A->00	(0*21)MOD 26	00->A
E->04	(4*21)MOD 26	06->G
H->07	(7*21)MOD 26	17->R
U->20	(20*21)MOD 26	04->E
A->00	(0*21)MOD 26	00->A
R->17	(17*21)MOD 26	19->T
K->10	(10*21)MOD 26	02->C
S->18	(18*21)MOD 26	14->O
W->22	(22*21)MOD 26	20->U
N->13	(13*21)MOD 26	13->N
R->17	(17*21)MOD 26	19->T
H->07	(7*21)MOD 26	17->R
Q->16	(16*21)MOD 26	24->Y

Finally we will get the original plaintext
"INDIA IS A GREAT COUNTRY".

Advantages: The Advantages of combining multiplicative cipher and keyed transposition cipher are:-

(1) More difficult to decrypt the combined code, due to the multiple encryption process.

(2) Overcome all the limitations of keyed cipher and multiplicative cipher.

(3) Brute force attack cannot easily crack the cipher code.

Disadvantages: The disadvantages of combining multiplicative substitution cipher and keyed transposition cipher are:-

(1) More difficult to remember the keys, used in both the approaches along with the inverse of keys being used

(2) It will take slight longer time to decrypt the code.

Conclusion: In the earlier approaches when multiplicative cipher and keyed transposition cipher were used separately there were chances of getting the code cracked by the third party.

After analyzing both of these techniques we came to the conclusion that neither of the technique is much secure. But a combination of both of these techniques can provide much better security than the security they provide alone. The main innovation in this paper is that this is the first time keyed transposition cipher and multiplicative substitution cipher are combined

to provide higher stability in the face of attacks, common in this area.

Acknowledgment: We would like to express our gratitude to Chitkara University and ICMES-2014 who gave us the priceless opportunity to present this research paper. We extremely express our profound gratitude to our HOD Dr. Deepak Arora and our faculty guide Mr.Bramah Hazela who have been a source of perpetual inspiration to us and gently guiding and paving us way towards a bright career.

References:

1. Behrouz A Forouzan “Cryptography and Network Security”,second edition McGraw-Hill.
2. William Stalling “Network Security Essentials (Applications and Standards)”,Pearson Education,2004.
3. Atul Kahate (2009),Cryptography and Network Security, second edition, McGraw-Hill.
4. Simmons, G. "Symmmetric and asymmetric encryption", *Computing Surveys*, vol. 11, December 1979, 305-330.
5. International Journal of Scientific & EngineeringResearch,Volume 1,Issue 2,November-2010 .

* * *

Student, Assistant Professor,Student,
Department of Computer Science, Amity University, Lucknow, India
prateek.1809@gmail.com,bramah_hazela@yahoo.com
Scienceshishirshukla164@gmail.com