Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementation of Affine Substitution Cipher with Keyed Transposition Cipher for Enhancing Data Security

Shishir Shukla
Department of Computer Science
Amity University, India

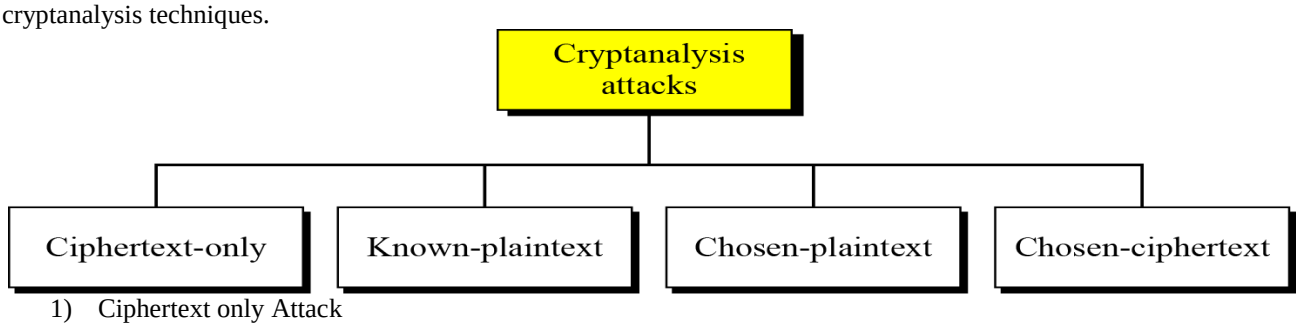
Prabhat Kumar Verma
Department of Computer Science
Amity University, India

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 Affine substitution cipher and Keyed transposition cipher techniques are used individually, cipher text obtained is easy to crack. Combining Affine substitution cipher with Keyed transposition cipher can eliminate their fundamental weakness and produce a cipher text that is hard to crack.

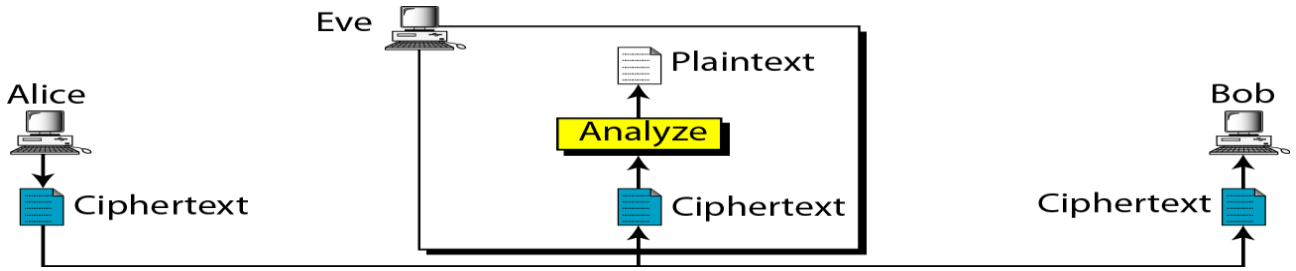
Keywords— Cryptography, Cipher Text, Cryptanalysis, Substitution, Transposition, Affine Cipher, Keyed Cipher.

I. INTRODUCTION

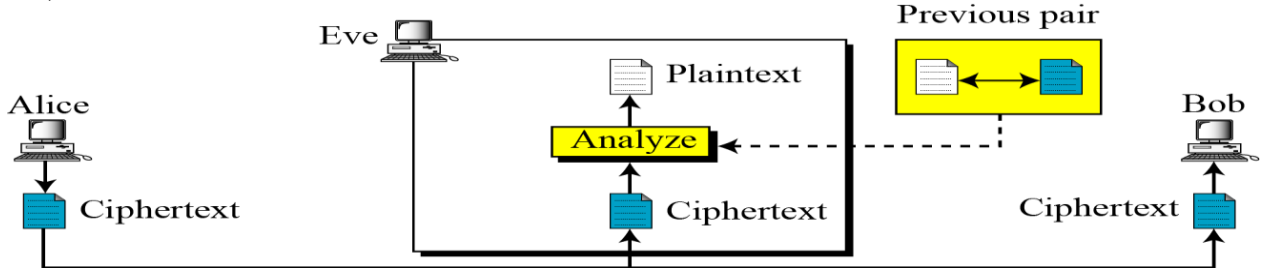
The requirements of information security within an organization have undergone major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. Cryptography, 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 is the science and art of breaking those codes. In addition to studying cryptography techniques, we also need to study cryptanalysis techniques.



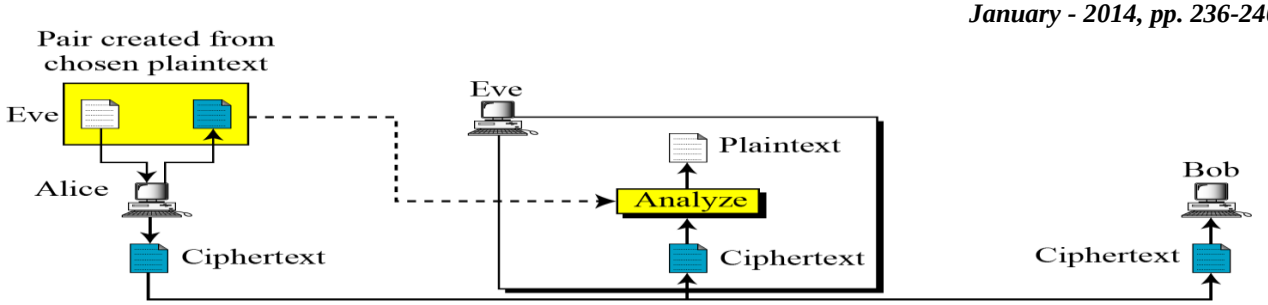
1) Ciphertext only Attack



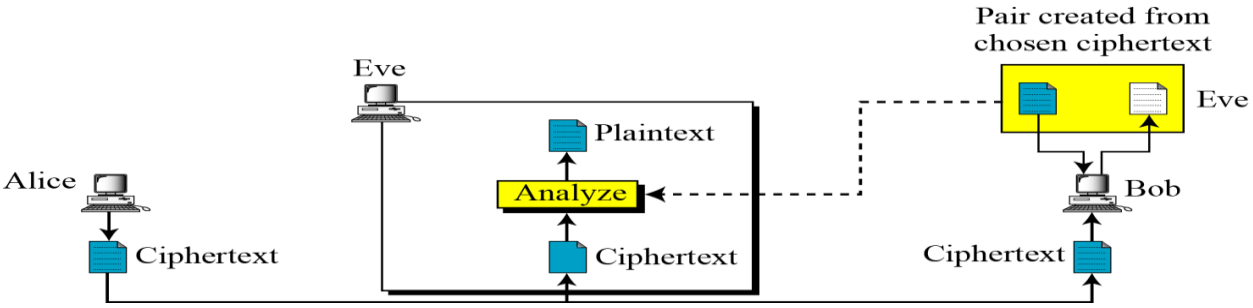
2) Known-Plaintext Attack



3) Chosen-Plaintext Attack



4) Chosen-Ciphertext Attack



II. THEORETICAL APPROACH

1) AFFINE SUBSTITUTION CIPHER

The **affine cipher** is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. Each letter is enciphered with the function (ax+b)mod 26 where b is the magnitude of the shift. In the affine cipher the letters of an alphabet of size are first mapped to the integers in the range . It then uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that correspond to a ciphertext letter. The encryption function for a single letter is

$$\mathrm{E}(x) = (ax + b) \mod m,$$

where modulus is the size of the alphabet and and are the key of the cipher. The value must be chosen such that and are co-prime. The decryption function is

$$\mathrm{D}(x) = a^{-1}(x - b) \mod m,$$

where a^{-1} is the modular multiplicative inverse of a modulo m . i.e., it satisfies the equation

$$1 = aa^{-1} \mod m.$$

2) KEYED TRANSPOSITION CIPHER

A **Transposition** Cipher is a rearrangement of the letters in the plaintext according to some specific system & key (i.e. a permutation of the plaintext). The most common of these are rectangular columnar transposition. **Steps of Rectangular Columnar Transposition are:**

1) Arrange horizontally in a rectangle.
2) Use a key to generate a permutation of the columns
3) Read vertically.

Suppose the key is of the order: 6 1 2 5 3 4 and the plaintext is: SELL ALL THE STOCKS ON MONDAY then

6	1	2	5	3	4
S	E	L	L	A	L

L	T	H	E	S	T
O	C	K	S	O	N
M	O	N	D	A	Y

Now the ciphertext would be: ETCO LHKN ASOA LTNY LESD SLOM.

Algorithm for Key Implementation in a keyed Transposition cipher is given below:

```
Given: EncKey [index]
index  ← 1
while (index ≤ Column)
  {
    DecKey[EncKey[index]] ← index
    index ← index + 1
  }
Return : DecKey [index]
```

III. PROPOSED WORK

In the proposed method we will combine affine substitution cipher with the keyed transposition cipher.

(A) ENCRYPTION ALGORITHM[1]

Step 1:- Take the plaintext as input and encrypt it by using the affine substitution cipher technique using two different pair of keys K1 and K2.
Step 2:- Pass the ciphertext values to keyed transposition cipher technique, where they will be arranged in a rowwise manner.
Step 3:- Assume the key for the encryption and decryption process.
Step 4:- Replace the columns, according to the assumed key.
Step 5:- Read the data in the columnwise manner.

(B) DECRYPTION ALGORITHM[2]

Step 1:- Read the data rowwise and arrange it columnwise.
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 rowwise manner.
Step 5:- Use the ciphertext values and the inverse of the key to get the required plaintext.

IV. IMPLEMENTATION[3]

ENCRYPTION STEPS[4]

Step 1:- Suppose we want to implement these two algorithms for the original message" I LOVE MY COUNTRY A INDIA". For this purpose we are using the length of key K1=5 and K2=2. So the value of $K1^{-1}$ will be 21. In case of encryption, the desired ciphertext value would be obtained by the formula

C=((P*K1)+K2)MOD26

Where C stands for ciphertext value, P stands for original plaintext value and K is the key value chosen by the original sender of the message.

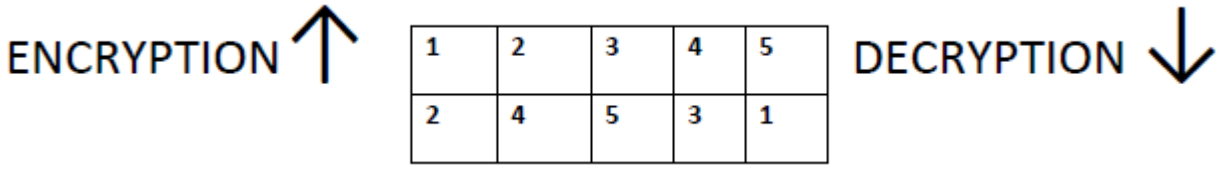
PLAINTEXT(P)	ENCRYPTION(E)	CIPHERTEXT(C)
I->08	((8*5)+2))MOD26	16->Q
L->11	((11*5)+2))MOD26	05->F
O->14	((14*5)+2))MOD26	20->U
V->21	((21*5)+2))MOD26	03->D
E->04	((4*5)+2))MOD26	22->W
M->12	((12*5)+2))MOD 26	10->K
Y->24	((24*5)+2))MOD 26	18->S
C->02	((2*5)+2))MOD 26	12->M
O->14	((14*5)+2))MOD 26	20->U
U->20	((20*5)+2))MOD 26	24->Y
N->13	((13*5)+2))MOD 26	15->P

T->19	((19*5)+2))MOD 26	19->T
R->17	((17*5)+2))MOD 26	09->J
Y->24	((24*5)+2))MOD 26	18->S
A->00	((0*5)+2))MOD 26	02->C
I->08	((8*5)+2))MOD 26	16->Q
N->13	((13*5)+2))MOD 26	15->P
D->03	((3*5)+2))MOD 26	17->R
I->08	((8*5)+2))MOD 26	16->Q
A->00	((0*5)+2))MOD 26	02->C

Step 2:- Now these Ciphertext values will be passed on to the Keyed Transposition Approach where first of all they will be arranged in a row wise format as shown below:

Q	**F**	**U**	**D**	**W**
K	**S**	**M**	**U**	**Y**
P	**T**	**J**	**S**	**C**
Q	**P**	**R**	**Q**	**C**

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



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

F	**D**	**W**	**U**	**Q**
S	**U**	**Y**	**M**	**K**
T	**S**	**C**	**J**	**P**
P	**Q**	**C**	**R**	**Q**

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

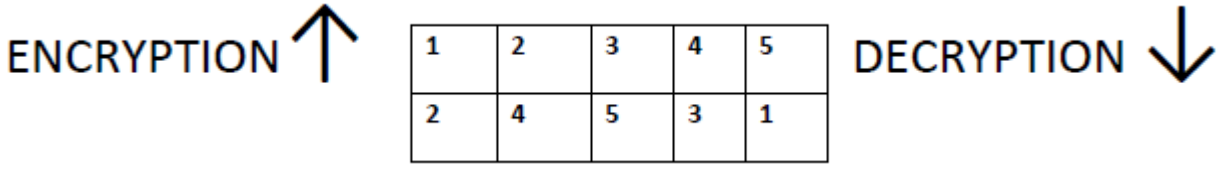
F	**S**	**T**	**P**	**D**	**U**	**S**	**Q**	**W**	**Y**
C	**C**	**U**	**M**	**J**	**R**	**Q**	**K**	**P**	**Q**

DECRYPTION STEPS[5]

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

F	**D**	**W**	**U**	**Q**
S	**U**	**Y**	**M**	**K**
T	**S**	**C**	**J**	**P**
P	**Q**	**C**	**R**	**Q**

Step 2:- Use the assumed key for the encryption and decryption process but will be used in a different manner.



The first column would be replace by fifth column, the fifth column would be replaced by third column, the third column would be replaced by fourth column, the fourth column would be replaced by second column and finally the second column would be replaced by first column. Hence,

Q	**F**	**U**	**D**	**W**
K	**S**	**M**	**U**	**Y**
P	**T**	**J**	**S**	**C**
Q	**P**	**R**	**Q**	**C**

Step 3:- Arrange the values in the row wise manner

Q	**F**	**U**	**D**	**W**	**K**	**S**	**M**	**U**	**Y**
P	**T**	**J**	**S**	**C**	**Q**	**P**	**R**	**Q**	**C**

Step 4:- We will get the plaintext values by using the formula

$$\mathbf{P=((C-K2)*K1^{-1}))mod26}$$

where the C will be ciphertext value obtained from the last step and K^{-1} will be the inverse of the key used. 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)
Q->16	((16-2)*21)MOD 26	08->I
F->05	((5-2)*21)MOD 26	11->L
U->20	((20-2)*21)MOD 26	14->O
D->03	((3-2)*21)MOD 26	21->V
W->22	((22-2)*21)MOD 26	04->E
K->10	((10-2)*21)MOD 26	12->M
S->18	((18-2)*21)MOD 26	24->Y
M->12	((12-2)*21)MOD 26	02->C
U->20	((20-2)*21)MOD 26	14->O
Y->24	((24-2)*21)MOD 26	20->U
P->15	((15-2)*21)MOD 26	13->N
T->19	((19-2)*21)MOD 26	19->T
J->09	((9-2)*21)MOD 26	17->R
S->18	((18-2)*21)MOD 26	24->Y
C->02	((2-2)*21)MOD 26	00->A
Q->16	((16-2)*21)MOD 26	08->I
P->15	((15-2)*21)MOD 26	13->N
R->17	((17-2)*21)MOD 26	03->D
Q->16	((16-2)*21)MOD 26	08->I
C->02	((2-2)*21)MOD 26	00->A

Finally we will get the original plaintext message" I LOVE MY COUNTRY A INDIA".

V. ADVANTAGES AND DISADVANTAGES

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

(1) More difficult to decrypt the combined code, due to the multiple encryption process used simultaneously with the pair of keys K1 and K2[6]
(2) Overcome all the limitations of keyed cipher and affine cipher as their individual approach.

The disadvantages of combining affine cipher and keyed transposition cipher are:-

(1) More difficult to remember the keys, used in both the approaches as in alone affine cipher two individual pair of keys are used as K1 and K2[7]
(2) It will take slight longer time to decrypt the code.

VI. CONCLUSION

In the earlier approaches when affine cipher and keyed transposition ciphers were used separately there were chances of getting the code being 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. When both of them are used in one approach individually they tend to be more powerful and economical. The main innovation in this paper is that this is the first time keyed transposition cipher and affine substitution cipher are combined to provide higher stability in the face of attacks, common in this area.

REFERENCES

[1] Adam, J."Threats and countermeasures", *IEEE Spectrum*, vol.29, August 1992, 21-28.

[2] Anderson,J.”A unification of computer and network security concepts”, *Proc.IEEE Symp. On Security and Privacy*, 1997, 65-71.
[3] Bell,T.” Technology1996: Communications”, *IEEE Spectrum*, vol.33, January 1996, 30-31.
[4] DeMillo, R. and Merritt,M.” Protocols for data security”, *IEEE Computer*, vol.16, February 1983, 39-54.
[5] Evans,A.et.al, “Comparing information without leaking IT”, *Commn. Of the ACM*, Vol.39, May 1996, 77-85.
[6] Hellman, M."An overview of public key cryptography",*IEEE communication society Magazine*, vol. 16,Novermber 1978, 24-32.
[7] Householder, A, et . al "Computer attack trend challenge internet security." *IEEE Computer and Privacy* 2002 Supplement,April 2002.

