Terna Engineering College

Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A: TO BE REFERRED BY STUDENTS)

Experiment No.01

A.1 Aim:

Design and Implementation of a product cipher using Substitution and Transposition ciphers.

A.2 Prerequisite:

1. Basic Knowledge of Cryptography.
2. Knowledge of Substitution Cipher techniques.

A.3 Outcome:

After the successful completion of this experiment, students will be able to apply the knowledge of symmetric cryptography to implement simple ciphers.

A.4 Theory:

- **Cryptography** is the art of achieving security by encoding messages to make them non-readable.

There are two types of cryptographic algorithms:

- **Substitution and**
- **Transposition**.

Product cipher is a combination of both these types to achieve a better effect of security.

An original message is known as the **plaintext**, while the coded message is called the **ciphertext.**

The process of converting from plaintext to ciphertext is known as enciphering or **encryption**; restoring the plaintext from the ciphertext is **deciphering or decryption**.

The many schemes used for encryption constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system or a cipher.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**.

Cryptanalysis is what the layperson calls "breaking the code."The areas of **cryptography and cryptanalysis together are called cryptology**.

- Cryptography is the art of achieving security by encoding messages to make them non-readable. There are two types of cryptographic algorithms: Substitution and Transposition. Product cipher is a combination of both these types to achieve a better effect of security.
- **Substitution Cipher:** Additive or Shift or Caesar Cipher algorithm is a cryptographic algorithm invented by Caesar. It is a substitution based algorithm.

• Symmetric Cipher Model

A symmetric encryption scheme has five ingredients (Figure 2.1):

• **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

• **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

• **Secret key:** The secret key is also input into the encryption algorithm. The key is a value independent of the plaintext and the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is a random stream of data and, as it stands, is unintelligible.

• **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

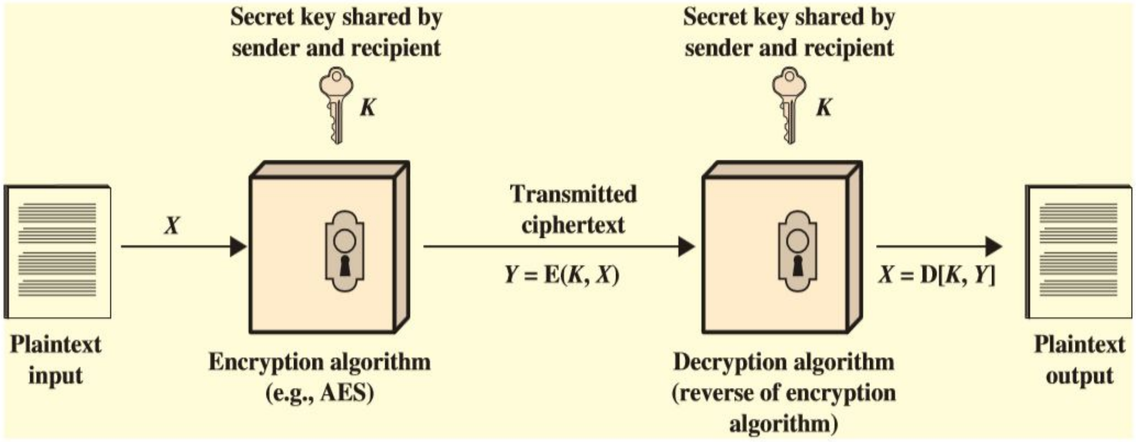

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D[K, Y]$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Symmetric Encryption

There are two requirements for the secure use of conventional encryption:

1. We need a robust encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a more vital form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she has several ciphertexts together with the plaintext that produced each ciphertext.

2. The sender and receiver must have obtained copies of the secret key securely and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

   We assume that it is impractical to decrypt a message based on the ciphertext plus knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret.

   This feature of symmetric encryption is what makes it feasible for widespread use. The fact that the algorithm need not be kept secret means that manufacturers can and have developed low-cost chip implementations of data encryption algorithms.

   These chips are widely available and incorporated into several products. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

Let us take a closer look at the essential elements of a symmetric encryption scheme, using Figure 2.2. A source produces a message in plaintext, X=[X1, X2, X3, ..., Xm].

The M elements of X are letters in some finite alphabet. Traditionally, the alphabet usually consisted of 26 capital letters. Nowadays, the binary alphabet {0, 1} is typically used.

For encryption, a key of the form K=[K1, K2, K3,......, Kj] is generated. If the key is generated at the message source, then it must also be provided to the destination employing some secure channel.

Alternatively, a third party could generate the key and securely deliver it to both source and destination.

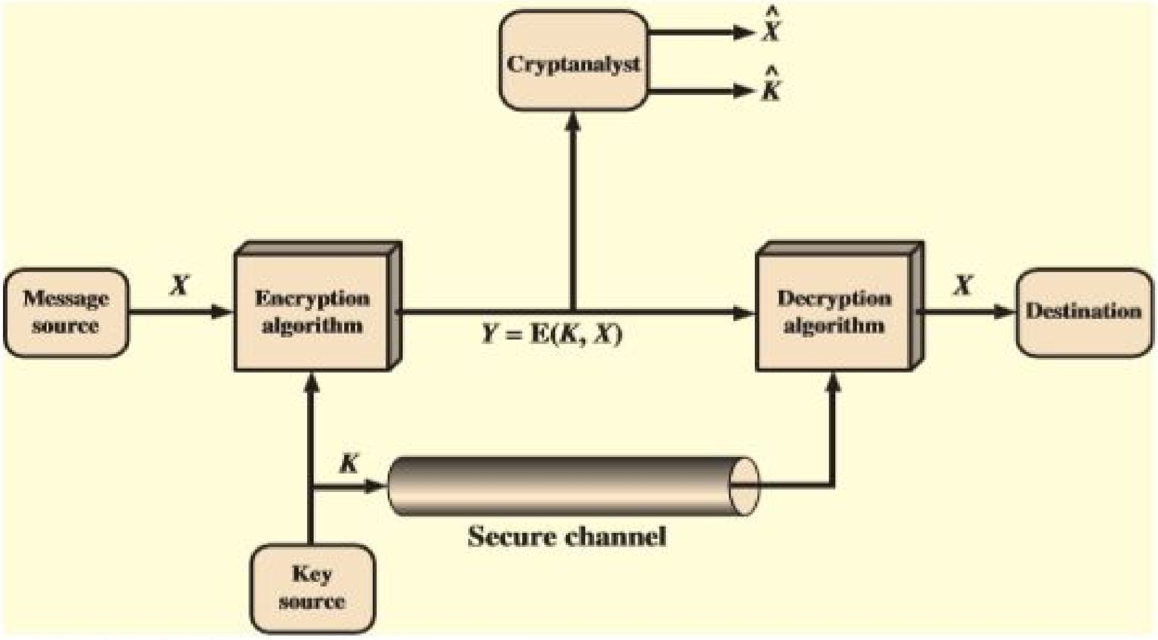


Figure 2.2 Model of Symmetric Cryptosystem

With the message and the encryption key K as input, the encryption algorithm forms the ciphertext Y=[Y1, Y2, Y3,..........., Yn]. We can write this as;

Y=E(K, X)

This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K.

The intended receiver, in possession of the key, can invert the transformation:

X=D(K,Y)

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K.It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover X by generating a plaintext estimate X. Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate K.

A.5 EXAMPLE:

1. Plaintext: CryPto(Sender's input)

   Key: 5(agreement key, here input)

   Cipher text: (C+5)(r+5)(y+5)(P+5)(t+5)(o+5)

   : HwdUyt(output)

2. Cipher Text: XdkcZm(Receiver's Input)

   Key: 5(agreement key, here input)

   Plaintext: CiphEr (output)

A.6 ALGORITHM:

@Encryption.....

A - Substitution Cipher

1. Take the Value of Plaintext.
2. Take Value of Key.
3. Run the loop n times here n will be the length of the text.
4. Convert the string into characters and that same time add with Key.
5. After Addition, mod 26 or 125 can be used depending on where you want to limit that entry of plain text.
6. Then save and convert the calculated part (character) into a string or StringBuffer.
7. Now the Final output will be the actual Cipher Text.

B - Transposition Cipher

1. The input of this Cipher will be the output from the Substitution Cipher.
2. Convert into a matrix with the help of the key (the key is different these times).
3. And with the help of the matrix, just lay down the content of the matrix or save the content into a simple string.
4. This String will be the Cipher Text.

@Decryption.....

Now out steps will be in reverse order.
Hence.
A - Transposition Cipher-

1. Input here will be the ciphertext.
2. Take Value of Key.
3. Insert this Cipher Text into the Transposition Cipher the whole algorithm remains the same.

   It just the value of k will change (k = cipher text/k).
4. Collect the characters and build them into a string.
5. That String will act as text that will be later interested in Substitution for the final decryption.

B - Substitution Cipher

1. After taking the input.
2. Use the same key.
3. Follow the Same producer as encryption, here the only difference is that instead of addition we will perform subtraction with the help of the key.
4. The result will be the Plain Text. And the code is finally decrypted.

PART B

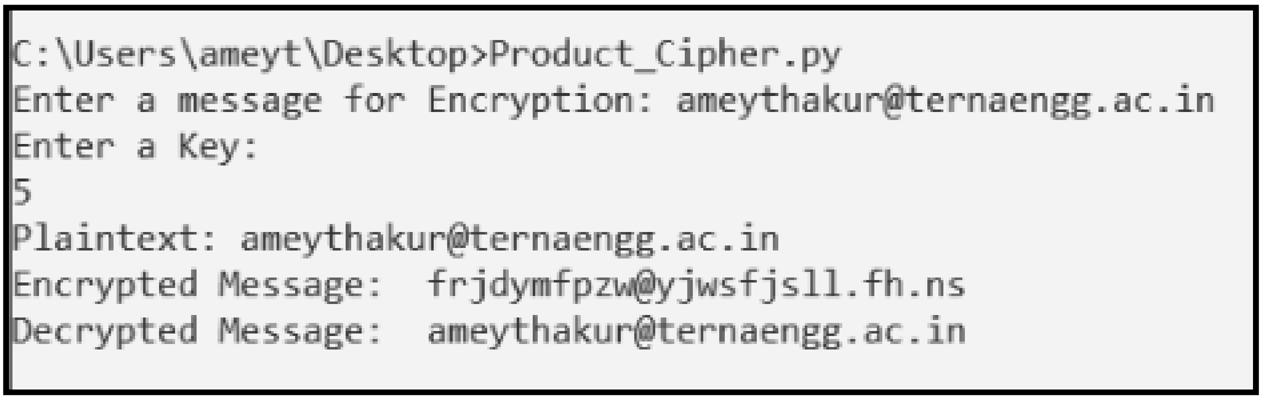
(PART B: TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)

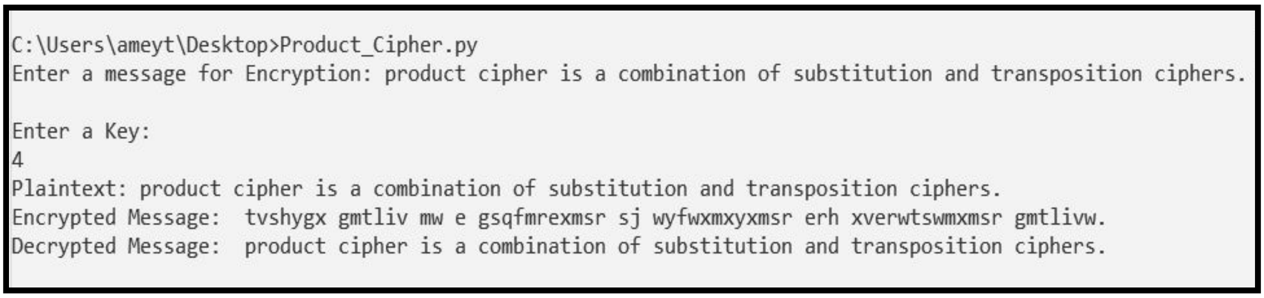
Roll No. 50	**Name:** AMEY THAKUR
Class: Comps TE B	**Batch:** B3
Date of Experiment: 29/01/2021	**Date of Submission:** 29/01/2021
Grade:	

B.1 The output of Product Cipher:

(add a snapshot of the output of product cipher)

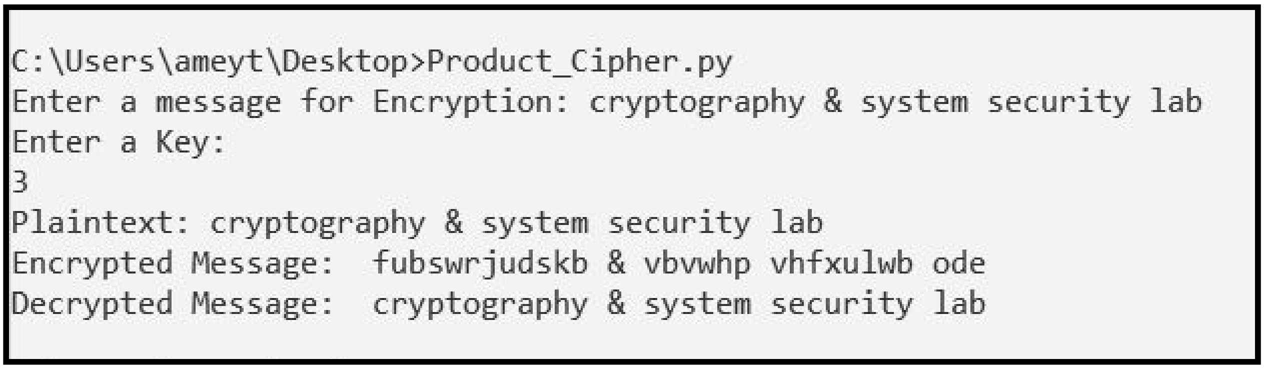


```
C:\Users\ameyt\Desktop>Product_Cipher.py
Enter a message for Encryption: ameythakur@ternaengg.ac.in
Enter a Key:
5
Plaintext: ameythakur@ternaengg.ac.in
Encrypted Message:  frjdymfpzw@yjwsfjsll.fh.ns
Decrypted Message:  ameythakur@ternaengg.ac.in
```



```
C:\Users\ameyt\Desktop>Product_Cipher.py
Enter a message for Encryption: product cipher is a combination of substitution and transposition ciphers.

Enter a Key:
4
Plaintext: product cipher is a combination of substitution and transposition ciphers.
Encrypted Message:  tvshygx gmtliv mw e gsqfmrexmsr sj wyfwxmxyxmsr erh xverwtswmxmsr gmtlivw.
Decrypted Message:  product cipher is a combination of substitution and transposition ciphers.
```



```
C:\Users\ameyt\Desktop>Product_Cipher.py
Enter a message for Encryption: cryptography & system security lab
Enter a Key:
3
Plaintext: cryptography & system security lab
Encrypted Message:  fubswrjudskb & vbvwhp vhfxulwb ode
Decrypted Message:  cryptography & system security lab
```

B.2 Source Code of Product Cipher:

(Add source code of product Cipher)

Product_Cipher.py

```
key = 'abcdefghijklmnopqrstuvwxyz'

def encrypt(n, plaintext):
   result = ''

   for l in plaintext.lower():
      try:
         i = (key.index(l) + n) % 26
         result += key[i]
      except ValueError:
         result += l

   return result.lower()

def decrypt(n, ciphertext):
   result = ''

   for l in ciphertext:
      try:
         i = (key.index(l) - n) % 26
         result += key[i]
      except ValueError:
         result += l

   return result

text=input(str("Enter a message for Encryption: "))
print("Enter a Key: ")
offset=input()
offset=int(offset,10)

print ("Plaintext: " + text)
encrypted = encrypt(offset, text)
print('Encrypted Message: ', encrypted)

decrypted = decrypt(offset, encrypted)
print('Decrypted Message: ', decrypted)
```

B.3 Question of Curiosity:

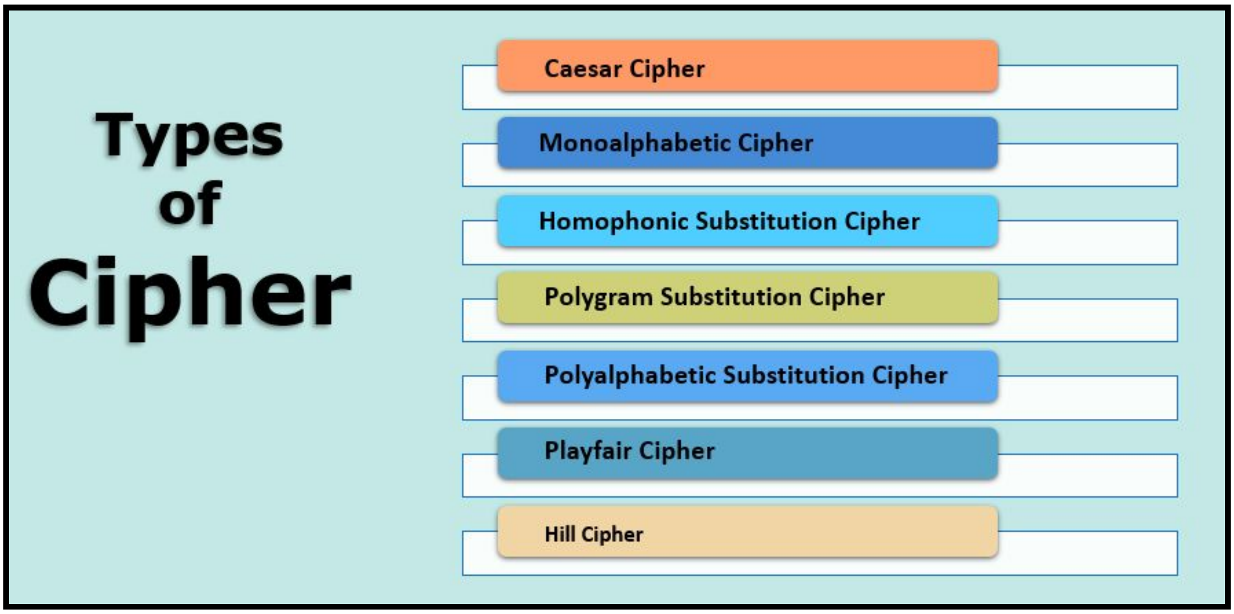
1. What are the Ciphers?

Ans:

- ➔ Cipher is a method to implement encryption and decryption of messages travelling in a network. It is used to increase the confidentiality of the messages.
- ➔ In cryptology, the discipline concerned with studying cryptographic algorithms, a cipher is an algorithm for encrypting and decrypting data. Symmetric key encryption, also called secret key encryption, depends on ciphers' use, which operates symmetrically. With symmetric algorithms, the same cipher and encryption keys are applied to data in the same way, whether the objective is to convert plaintext to ciphertext or ciphertext to plaintext. A cipher transforms information by processing the original plaintext characters (or other data) into ciphertext, which should be random.
- ➔ Traditionally, ciphers used two main types of transformation: transposition ciphers, which keep all the original bits of data in a byte but mix their order, and substitution ciphers, which replace specific data sequences with other specific data sequences. For example, one type of substitution would be to transform all bits with a value of 1 to a value of 0, and vice versa. The data output by either method is called the ciphertext.
- ➔ Modern ciphers enable private communication in many different networking protocols, including the Transport Layer Security (TLS) protocol and others that offer network traffic encryption. Many communication technologies, including phones, digital television, and ATMs, rely on ciphers to maintain security and privacy.

2. What are the different types of Cipher?

Ans:


Types of Cipher
Caesar Cipher
Monoalphabetic Cipher
Homophonic Substitution Cipher
Polygram Substitution Cipher
Polyalphabetic Substitution Cipher
Playfair Cipher
Hill Cipher

Types of Cipher

Several types of cipher are given as follows:

1. Caesar Cipher

➔ In Caesar cipher, the set of characters of plain text is replaced by any other character, symbols, or numbers. It is a very weak technique of hiding text. In Caesar's cipher, each alphabet in the message is replaced by three places down. Let's see one example. The plain text is EDUCBA. As a Caesar cipher, each alphabet is replaced by three-place down, so E will replace by H, D will replace by G, U will replace by X, C will replace by F, B will replace by E and A will replace by D. So here the plain text is EDUCBA and ciphertext Is HGXFED.

➔ Caesar cipher algorithm is as follows:

1. Read each alphabet of plain text.
2. Replace each alphabet with 3 places down.
3. Repeat the process for all alphabet in plain text.

➔ A Modified Version of Caesar Cipher: This cipher works the same as Caesar cipher, the only difference is – in Caesar cipher, each alphabet is replaced by three-place down wherein a modified version of Caesar cipher, the number is decided by a user to replace the alphabet and this number will be constant. For example, EDUCBA and number for the replacement are 1, so E will replace by F, D will replace by E, U will replace by V, C will replace by D, B will replace by C and A will replace by B. So here the plain text is EDUCBA and ciphertext Is FEVDCB.

➔ A modified version of the Caesar cipher algorithm is as follows

1. Read each alphabet of plain text.
2. Take the number for replacement.
3. Replace each alphabet with a specified number down.
4. Repeat the process for all alphabet in plain text.

2. Monoalphabetic Cipher

➔ As Caesar cipher and a modified version of Caesar cipher is easy to break, a monoalphabetic cipher comes into the picture. In monoalphabetic, each alphabet in plain text can be replaced by any other alphabet except the original alphabet. That is A can be replaced by any other alphabet from B to Z. B can be replaced by A or C to Z. C can be replaced by A, B, and D to z, etc.

➔ Mono alphabetic cipher causes difficulty to crack the message as there are random substitutions and a large number of permutations and combinations are available.

3. Homophonic Substitution Cipher

➔ A homophonic substitution cipher is similar to a monoalphabetic cipher the only difference is in monoalphabetic we replace the alphabet with any other random alphabet except the original alphabet wherein homophonic substitution cipher, the alphabet is replaced by fixed alphabet or set of alphabet. The substitution alphabet is replaced with the fixed.

➔ For example, replace A with x, E with B, S with A, etc., or replace A with E, x or L, B with T, A, Z, etc.

4. **Polygram Substitution Cipher**

➔ In polygram substitution cipher, rather than replacing each alphabet with another, the Block of alphabets is replaced with another block of alphabets. Replace EDUCBA with XYQLAB. In this case, EDUCBA will be replaced with XYQLAB, but EDU can be replaced with another set of the block, let's assume EDU will replace LOD. In this type of ciphers, the replacement of plain text is done through the block by block rather than character by character.

5. **Polyalphabetic Substitution Cipher**

➔ Polyalphabetic Cipher is also known as Vigenere Cipher which is invented by Leon Battista Alberti. In Polyalphabetic Substitution Cipher is a method of encrypting alphabetic texts. It uses multiple substitution alphabets for encryption. Vigenere square or Vigenere table is used to encrypt the text. The table contains 26 alphabets written in different rows each alphabet being cyclically shifted to the left following the previous alphabet, equivalent to the 26 possible Caesar Ciphers. The cipher uses a different alphabet from one of the rows at various points in the encryption process.

➔ Let's consider Original text is Educba and the keyword is Apple. For the encryption process, The first letter of the original text, E is paired with A, the first letter of the key. So use row E and column A of the Vigenère square, which is E. Similarly, for the second letter of the original text, the second letter of the key is used, the letter at row d and column p is s. The rest of the original text is enciphered in the same way. The final encryption of Educba is Esjnfa.

6. **Playfair Cipher**

➔ Playfair cipher is also called Playfair square. It is a cryptographic technique that is used to encrypt the data.

➔ The Playfair cipher process is as follows:

    1. Creation and population of the matrix.
    2. Encryption process.

➔ Let's discuss the above-mentioned steps in detail: manners, creation and population of the matrix. It uses a 5 * 5 matrix to store the keyword or the key which is used for the encryption and decryption process.

➔ This step is working as follows:

    1. Enter the keyword in the matrix in a row-wise manner i.e., from left to right and top to bottom.
    2. Skip the duplicate words in the keyword.
    3. Fill the remaining spaces with the rest of the alphabets (A – Z) that were not a part of the keyword.

Note: while doing so, combine I and J in the same cell of the table. i.e. If I or J is present in the keyword, discard both I and J while filling the remaining space encryption process.

➔ The encryption process works as follows:

1. Break the alphabets into groups (each group must contain two values). The encryption processes will be performed on these groups.
2. If both alphabets in the group are the same, add x after the first alphabet.
3. If both the alphabet in the group are present in the same row of the matrix, replace them with the alphabets to their immediate right, respectively. If the original group is on the right side of the row, then wrapping around to the row's left side happens.
4. If both the alphabet in the group are present in the same column, replace them with the alphabet immediately below. If the original group is on the bottom side of the row, then wrapping around to the row's top side happens.
5. If both the alphabet in the group are not in the same row or column, replace them with the alphabets in the same row immediately but at the other pair of corners of the rectangle, defined by the original group.

7. Hill Cipher

➔ Hill cipher works on multiple alphabets at the same time. Hill cipher works as follows:

1. Assign the number to each alphabet in the plain text. A = 0, B= 1….z = 25.
2. Organize the plain text message as a matrix of numbers based on the above step that is in number format. The resultant matrix is called a plain text matrix.
3. Multiply the plain text matrix with a randomly chosen key. Note that the key matrix must be the size of n*n, where n stands for the number of rows in a plain text matrix.
4. Multiply both the matrix, i.e., step 2 and step 3.
5. Calculate the mod 26 value of the above matrix, i.e., matrix results in step 4.
6. Now translate the numbers to alphabets i.e. 0 =A, 1 =B, etc.
7. The result of step 6 becomes our ciphertext.

3. What is a Substitution Cipher? Explain with an example.

Ans:

Substitution Cipher

➔ A substitution cipher is a type of encryption where characters or units of text are replaced by others to encrypt a text sequence.

- ➔ Substitution ciphers are a part of early cryptography, predating the evolution of computers, and are now relatively obsolete.
- ➔ In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

Note: Special case of Substitution cipher is known as Caesar cipher where the key is taken as 3.

Mathematical representation

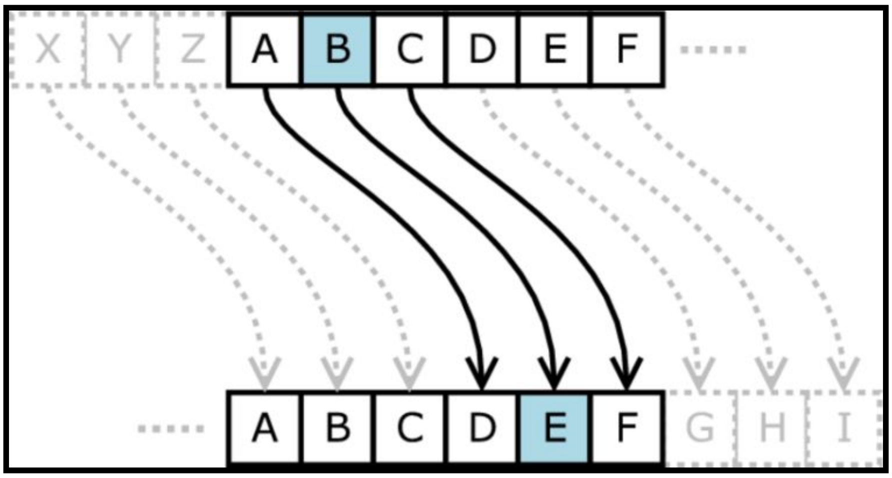
- ➔ The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.
- ➔ Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) \ = (x + n) mod\ 26$$

(Encryption Phase with shift n)

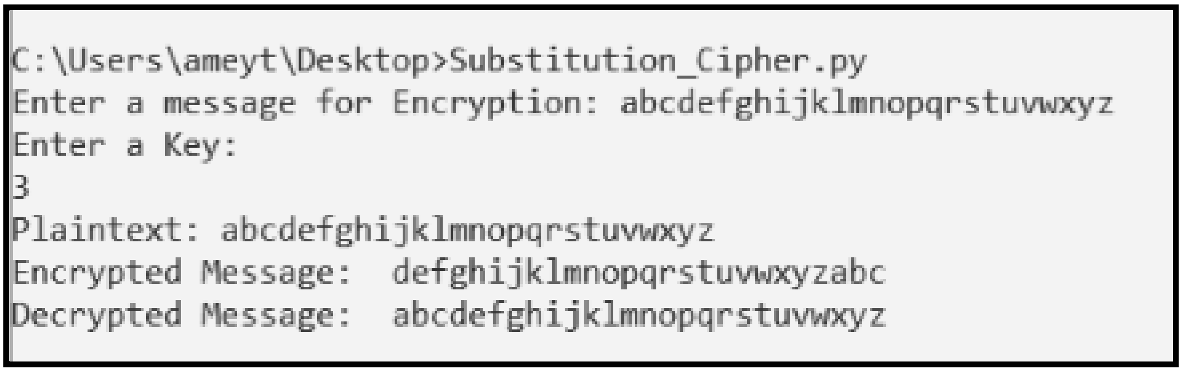
$$D_n(x) \ = (x - n) mod\ 26$$

(Decryption Phase with shift n)



Original: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shifted: DEFGHIJKLMNOPQRSTUVWXYZABC

Examples:



```
C:\Users\ameyt\Desktop>Substitution_Cipher.py
Enter a message for Encryption: abcdefghijklmnopqrstuvwxyz
Enter a Key:
3
Plaintext: abcdefghijklmnopqrstuvwxyz
Encrypted Message:  defghijklmnopqrstuvwxyzabc
Decrypted Message:  abcdefghijklmnopqrstuvwxyz
```

Algorithm for Substitution Cipher:

- ➔ Input:
  1. A String of both lower and upper case letters, called PlainText.
  2. An Integer is denoting the required key.
- ➔ Procedure:
  1. Create a list of all the characters.
  2. Create a dictionary to store the substitution for all characters.
  3. For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
  4. Print the new string generated.

4. What is a Transposition Cipher? Explain with an example.

Ans:

Transposition Cipher

- ➔ Transposition Cipher is a cryptographic algorithm where alphabets in the plaintext are rearranged to form a ciphertext. In this process, the actual plain text alphabets are not included.

Example

- ➔ A simple example for a transposition cipher is a columnar transposition cipher where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different ciphertext.
- ➔ Consider the plain text Amey Thakur, and let us apply the simple columnar transposition technique shown below.

ENCRYPTION

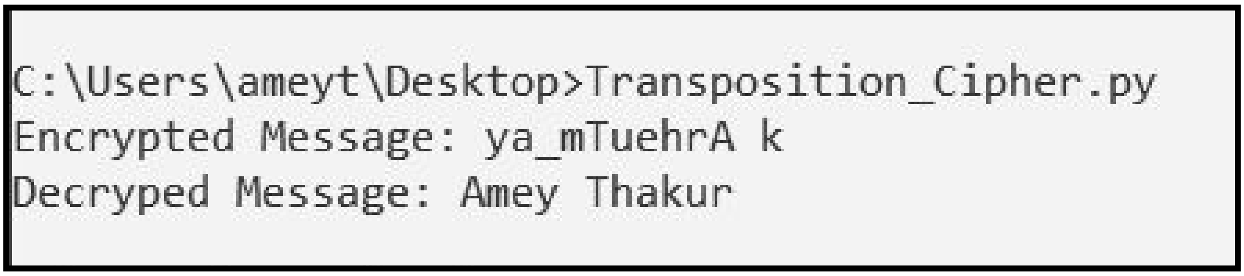
Given Text: Amey Thakur	**Keyword:** MEGA
Length of Keyword: 4(No. Of rows)	**Order of Alphabets in MEGA:** 4231

M	**E**	**G**	**A**
4	**2**	**3**	**1**
A	m	e	y
_	T	h	a
k	u	r	_

Print Characters of Column: 1,2,3,4.

Encrypted Text: ya_mTuehrA_k

Output:



```
C:\Users\ameyt\Desktop>Transposition_Cipher.py
Encrypted Message: ya_mTuehrA k
Decryped Message: Amey Thakur
```

DECRYPTION

1. The recipient has to work out the column lengths by dividing the message length by the key size to decipher it.
2. Then, write the message out in columns again, then re-order the columns by reforming the keyword.

5. Explain Affine Cipher.

Ans:

Affine Cipher

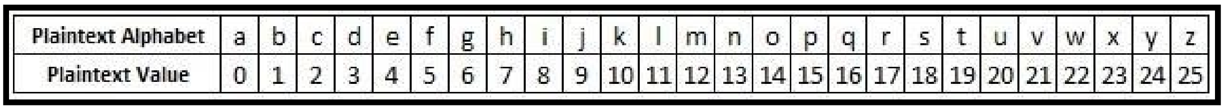
- The Affine Cipher is another example of a Monoalphabetic Substitution cipher. It is slightly different from the other models encountered here since the encryption process is substantially mathematical. The whole process relies on working modulo m (the length of the alphabet used). By performing a calculation on the plaintext letters, we encipher the plaintext.

Encryption

- The encryption process's first step is to transform each of the letters in the plaintext alphabet to the corresponding integer in the range 0 to m-1. With this done, the encryption process for each letter is given by

  $$E(x) = (ax + b) \bmod m$$

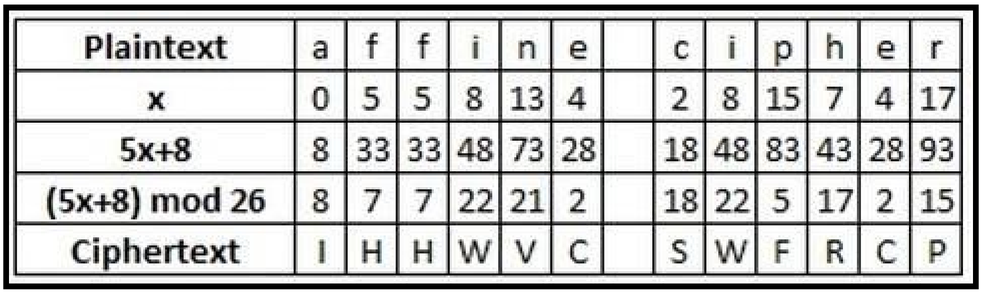
  A and b are the key for the cipher; this means that we multiply our integer value for the plaintext letter by adding b to the result. Finally, we take this modulus m (that is, we take the remainder when the solution is divided by m or take away the alphabet's length until we get a number less than this length).
- For example, let us encrypt the plaintext "affine cipher," using the key a = 5, b = 8. Firstly we must find the integer value of each of the letters in the plaintext alphabet (the standard alphabet of 26 letters in this case). The table below gives these values.



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The typical values for the alphabet of 26 letters. Notice we start at 0, not 1.

➔ With the integer values of the plaintext letters found, the next step is to perform the calculations on those values. In this instance, the math needed is (5x+8). Finally, we must ensure that all our answers are calculated mod 26 and convert the integers back to ciphertext letters. All this information is shown in the table below.



Plaintext	a	f	f	i	n	e		c	i	p	h	e	r
x	0	5	5	8	13	4		2	8	15	7	4	17
5x+8	8	33	33	48	73	28		18	48	83	43	28	93
(5x+8) mod 26	8	7	7	22	21	2		18	22	5	17	2	15
Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P

The affine cipher with a = 5, b = 8. We work out values of letters, then do the calculations before converting numbers back to letters.

➔ Thus the ciphertext produced is "IHHWVC SWFRCP.”

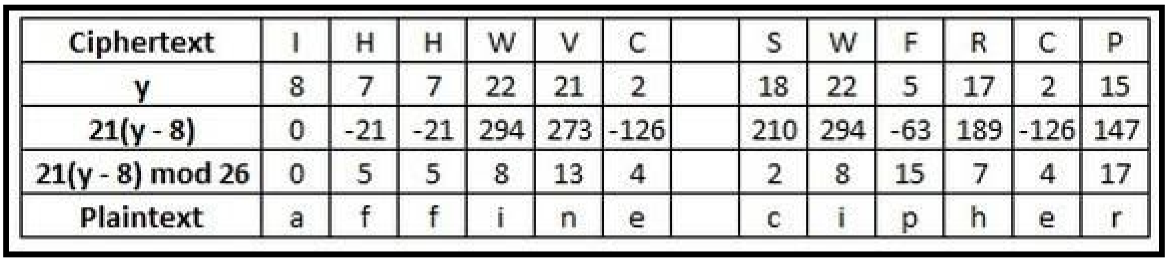
Decryption

➔ In deciphering the ciphertext, we must perform the opposite (or inverse) functions on the ciphertext to retrieve the plaintext. Once again, the first step is to convert each of the ciphertext letters into their integer values. We must now perform the following calculation on each integer.

$$D(x) = c(x - b) \bmod m$$

Where c is the modular multiplicative inverse of a, an x c = 1 mod m (c is the number such that when you multiply a by it and keep taking away the alphabet’s length, you get to 1).

➔ Continuing our example, we shall decrypt the ciphertext "IHHWVC SWFRCP,” using a key of a = 5, b = 8. The first step here is to find the inverse of a, which in this case is 21 (since 21 x 5 = 105 = 1 mod 26, as 26 x 4 = 104, and 105 - 104 = 1). We must now perform the inverse calculations on the integer values of the ciphertext. In this case, the calculation is 21(y - 8). Once again, we must take these answers modulo 26 and finally convert the integers back to plaintext letters. This is shown in the table below.



Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P
y	8	7	7	22	21	2		18	22	5	17	2	15
21(y - 8)	0	-21	-21	294	273	-126		210	294	-63	189	-126	147
21(y - 8) mod 26	0	5	5	8	13	4		2	8	15	7	4	17
Plaintext	a	f	f	i	n	e		c	i	p	h	e	r

The decryption process for a key of a = 5, b = 8. We had to find the inverse of a first, which is 21.

- ➔ We retrieve our plaintext of "affine cipher.”

B.4 Conclusion:

(Write an appropriate conclusion.)

After completing this experiment, we will be able to apply symmetric cryptography knowledge to implement simple ciphers. Also, we can now work with cryptology as we learned about various mathematical models and algorithms. We got an in-depth understanding of ciphers with the programs and mathematical implementation. This experiment helped to understand Plaintext, Encryption, and Decryption theory.