Academic Year: 2024-25	**Programme: BTECH-Cyber (CSE)**
Year: 2nd	**Semester: IV**
Student Name: Arjun Mehta	**Batch : K1**
Roll No: K036	**Date of experiment: 09-01-2025**
Faculty: Rejo Mathew	**Signature with Date:**

Experiment 2: Vigenere Cipher

Aim: To study and implement Vigenere Cipher.

Learning Outcomes:

After completion of this experiment, student should be able to

1. Understand steps of Vigenere Cipher.
2. Implement Vigenere Cipher.
3. Understand variations of Vigenere Cipher and its effectiveness.

Theory:

The Vigenére cipher is an example of polyalphabetic substitution cipher. This cipher uses multiple one-character keys. Each of the keys encrypts one plain-text character. The first key encrypts the first plain-text character; the second key encrypts the second plain-text character, and so on. After all the keys are used, they are recycled. Thus, if we have 30 one-letter keys, every 30th character in the plain text would be replaced with the same key. This number (in this case, 30) is called the period of the cipher.
The main features of polyalphabetic substitution cipher are the following:
(a) It uses a set of related monoalphabetic substitution rules.
(b) It uses a key that determines which rule is used for which transformation.

For example, let us discuss the Vigenére cipher, which is an example of this cipher. In this algorithm, 26 Caesar ciphers make up the mono-alphabetic substitution rules. There is a shifting mechanism, from a count of 0 to 25. For each plain-text letter, we have a correspondingsubstitution, which we call the key letter. To understand this technique, we need to take a lookat a table, which is formally known as Vigenére tableau.

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	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

The alphabet used at each point depends on a repeating keyword.

Input:

Plaintext: SEEINTHEMALL

Keyword : INFOSEC

Output:

Ciphertext: A R J W F X J M Z F Z D

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.

The keyword "INFOSEC" generates the key "INFOSECINFO"

The plain text is then encrypted using the process explained below.

Encryption

The first letter of the plaintext, S is paired with I, the first letter of the key. So use row S and column I of the Vigenere square, namely A. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column N is R. The rest of the plaintext is enciphered in a similar fashion.

Decryption

Using the table, choose the row corresponding to the keyword character and look for the ciphertext character in that row.Plaintext character is then at the top of that column

Input: *Ciphertext:* ARJAWMPUNQZ *Keyword:* INFOSEC

Output: *Plaintext:* SEEINTHEMALL

Mathematical Expression for Vigenere Cipher

Converting [A-Z] into numbers [0–25].

Encryption

The plaintext(P) and key(K) are added modulo 26.

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i + 26) \bmod 26$

Note: D_i denotes the offset of the i^{th} character of the plaintext. Like offset of A is 0 and of B is 1 and so on.

Steps to follow: Code has to be with comments

#Encryption

```
plaintext=input("Enter plain text: ")
keyword=input("Enter key: ")

key=(keyword*(len(plaintext)//len(keyword)))+keyword[:len(plaintext) % len(keyword)]

ciphertext=""
```

for i in range(len(plaintext)):

p=plaintext[i]

if p==' ':

ciphertext+=' '

else:

k=key[i]

p_val=ord(p.upper())-ord('A')

k_val=ord(k.upper())-ord('A')

encrypted_val=(p_val+k_val) % 26

encrypted_char=chr(encrypted_val+ord('A'))

ciphertext+=encrypted_char

print(f"Ciphertext is: {ciphertext}")

```
In [12]: #Encryption

plaintext=input("Enter plain text: ")
keyword=input("Enter key: ")

key=(keyword*(len(plaintext)//len(keyword)))+keyword[:len(plaintext) % len(keyword)]

ciphertext=""

for i in range(len(plaintext)):
    p=plaintext[i]
    if p==' ':
        ciphertext+=' '
    else:
        k=key[i]
        p_val=ord(p.upper())-ord('A')
        k_val=ord(k.upper())-ord('A')
        encrypted_val=(p_val+k_val) % 26
        encrypted_char=chr(encrypted_val+ord('A'))
        ciphertext+=encrypted_char

print(f"Ciphertext is: {ciphertext}")

Enter plain text: Arjun Mehta
Enter key: cyber
Ciphertext is: CPKYE KFLKC
```

#Decryption

ciphertext=input("Enter cipher to be decrypted: ")

keyword=input("Enter key: ")

key=(keyword*(len(ciphertext)//len(keyword)))+keyword[:len(ciphertext)%len(keyword)]

plaintext=""

for i in range(len(ciphertext)):

c=ciphertext[i]

if c==' ':

plaintext+=' '

else:

k=key[i]

c_val=ord(c.upper())-ord('A')

k_val=ord(k.upper())-ord('A')

decrypted_val=(c_val-k_val+26)%26

decrypted_char=chr(decrypted_val+ord('A'))

plaintext+=decrypted_char

print(f"Decrypted Text: {plaintext}")

```
In [13]: #Decryption

ciphertext=input("Enter cipher to be decrypted: ")
keyword=input("Enter key: ")

key=(keyword*(len(ciphertext)//len(keyword)))+keyword[:len(ciphertext)%len(keyword)]

plaintext=""

for i in range(len(ciphertext)):
    c=ciphertext[i]
    if c==' ':
        plaintext+=' '
    else:
        k=key[i]
        c_val=ord(c.upper())-ord('A')
        k_val=ord(k.upper())-ord('A')
        decrypted_val=(c_val-k_val+26)%26
        decrypted_char=chr(decrypted_val+ord('A'))
        plaintext+=decrypted_char

print(f"Decrypted Text: {plaintext}")

Enter cipher to be decrypted: CPKYE KFLKC
Enter key: cyber
Decrypted Text: ARJUN MEHTA
```

Questions:

1. Is the 16th century - Vigenere Cipher still worthy? Justify?
2. What is the common types of attacks on Vigenere Cipher?
3. Discuss the impact of the key length on the security of the Vigenère cipher. Why does a longer key generally provide better security?
4. What is difference of autokey method and keyword method of Vigenere Cipher?

1. **Is the 16th century - Vigenère Cipher still worthy? Justify?**
    - The Vigenère Cipher is no longer secure by modern standards because it can be broken with techniques like frequency analysis (Kasiski examination). However, it is still useful for educational purposes to understand encryption principles and cryptography basics.
2. **What are the common types of attacks on Vigenère Cipher?**
    - Common attacks on the Vigenère Cipher include:
        - **Frequency Analysis**: Analyzing the repetition of letters to break the cipher.
        - **Kasiski Examination**: Identifying repeating patterns in the ciphertext to guess the key length.
        - **Brute Force Attack**: Trying all possible key combinations, especially when the key is short.
3. **Discuss the impact of the key length on the security of the Vigenère cipher. Why does a longer key generally provide better security?**
    - A longer key provides better security because it reduces the frequency of repeated patterns in the ciphertext, making it harder to perform frequency analysis. With a longer key, the cipher becomes more resistant to cryptographic attacks, as the key doesn't repeat frequently.
4. **What is the difference between the autokey method and keyword method of Vigenère Cipher?**
    - **Keyword Method**: The key is repeated to match the length of the plaintext.
    - **Autokey Method**: The key is used only for the first letter, and then the plaintext itself is used as the key for the remaining letters. This reduces the repetition of the key, enhancing security.

Conclusion: Have understood and implemented the cipher of this lab successfully.