Question Number 7

Recall the Vigenre Cipher discussed in class.

- Encrypt MY HOME IS INDIA using a Vigenre Cipher with keyword KEA.
- The ciphertext JNHYSMCDJOP was obtained by encrypting an English word using a Vigenre Cipher:
  - The first and ninth letters of the plaintext are identical. What does this tell you about the key?
  - Given the keyword length is less than 7, the third and fourth letters of the plaintext are F and O, respectively, and A is a letter in the keyword, find the keyword and the plaintext.
- If the keyword of a Vigenre Cipher has repeated letters, does this make it any easier to break?

Solution.

Part1

Vigenre Cipher Table

Plain Text	M (12)	Y (24)	H (7)	O (14)	M (12)	E (4)	I (8)	S (18)	I (8)	N (13)	D (3)	I (8)	A (0)
Key	K (10)	E (4)	A (0)	K (10)	E (4)	A (0)	K (10)	E (4)	A (0)	K (10)	E (4)	A (0)	K (10)
Cipher Text	W (22)	C (2)	H (7)	Y (24)	Q (16)	E (4)	S (18)	W (22)	I (8)	X (23)	H (7)	I (8)	K (10)

Table 1: Vigenre Cipher

Part2.1

Given the ciphertext `JNHYSMCDJOP` obtained by encrypting an English word using a Vigenre cipher, and knowing that the first and ninth letters of the plaintext are identical, we can infer the following about the key:

Key Points

a) **Plaintext Repetition:**
The first and ninth letters of the plaintext are the same, $P_1 = P_9$.

b) **Ciphertext Repetition:**
The ciphertext letters corresponding to these positions are also identical, $C_1 = C_9$.

Since $P_1 = P_9$ and $C_1 = C_9$, it follows that:

$$(P_1 + K_1) \mod 26 = (P_9 + K_9) \mod 26$$

Given $P_1 = P_9$, it simplifies to:

$$K_1 \equiv K_9 \pmod{26}$$

c) The equality $K_1 = K_9$ indicates that the key must repeat every 8 characters or a divisor of 8 (1, 2, 4, 8) because the positions 1 and 9 are 8 characters apart.

d) If the key length is shorter than 8 characters, it must be a repeating key whose length divides 8. Thus, the key could be of lengths 1, 2, 4, or 8.

e) So we can conclued from observation that $P_1 = P_9$ and $C_1 = C_9$ provides a constraint on the key's periodicity. The key must repeat at intervals that align with the distance between these positions in the plaintext, giving us valuable insight into possible key lengths and their periodic patterns.

Part2.2

Given

- We Know key length is less than 7
- Also given thrid and fourth letters of plain text as 'F' and 'O'.
- Key contain letter 'A'

From above part we know that if key length is less than 8 then possible length of key is 1,2 and 4. So we can try all key of length 1,2 and 4 which contain letter 'A'.

Calculating the key for the 3rd and 4th positions

a) For the 3rd position:

- $C_3 = H$ (ciphertext) and $P_3 = F$ (plaintext)

Calculate the key:

$$K_3 = (C_3 - P_3) \mod 26 = (H - F) \mod 26 = (7 - 5) \mod 26 = 2$$

So, K_3 corresponds to the letter **C**.

b) For the 4th position:

- $C_4 = Y$ (ciphertext) and $P_4 = O$ (plaintext)

Calculate the key:

$$K_4 = (C_4 - P_4) \mod 26 = (Y - O) \mod 26 = (24 - 14) \mod 26 = 10$$

So, K_4 corresponds to the letter **K**.

From above result we can conclude that our key Contains letter A, C and K. Also we can discard the posibility of key length 1,2. So our key lenght is 4. Our key is in the following format

i *ACK

ii A*CK

We can try all possible keys to decrypt the given cipher text to plain text and find valid english word. To achieve this we use python code(`vigenre.py`) to iteratively eliminate invalid keys and find the correct one.

Note Before executing `vigenre.py` file make sure you have installed all requried libraries listed in `requirements.txt` using following command.

```
    pip install -r requirements.txt
```

After Executing Code We will get Plaintext and Key as follows

- Plaintext - > **INFORMATION**
- Key - > **BACK**

Part3

Yes, the presence of repeated letters in a Vigenère Cipher's keyword can indeed make it more susceptible to decryption. When a keyword contains repetitions, it introduces periodic patterns in the ciphertext. These patterns can be detected and analyzed using frequency analysis techniques. For example, if the keyword is repeating, the cipher effectively transforms into a series of Caesar ciphers, each with a shift determined by the corresponding letter of the keyword.

By identifying the repeating nature of the key, one can use methods such as the Kasiski examination to determine the length of the keyword. Once the length is known, the ciphertext can be segmented into multiple Caesar ciphers, each corresponding to a single position in the keyword. Analyzing the frequency of letters in these segments can then help in deducing the individual letters of the repeating key, leading to the eventual decryption of the plaintext.