Question Number 8

Encrypt the names of all members of your group with any three classical ciphers using Sage. Also write a case-study in cryptanalyzing any one of them. Do some research on this. Can you implement the cryptanalysis strategy you have chosen using Sage. The difficulty of the strategy you choose will decide the marks you score in this problem.

Solution. To Encrypt the names of all members of my group I have used Hill Cipher, Transposition Cipher, Vigenere Cipher. Below are the screenshot of code that show encryption of name using Sage.

```
sage:
sage: S = AlphabeticStrings()
sage: E = HillCryptosystem(S, 3)
sage: A = E.random_key()
sage: B = E.inverse_key(A)
sage: e = E(A)
sage: c = E(B)
sage:
sage:
sage: ## Encrypting group member name
sage:
sage: # Vedant
sage: M_ved = S("VEDANT")
sage: e(M_ved)
HMIQBX
sage:
```

```
sage:
sage: # Karan
sage: M_karan = S("KARANKUMBHAR")
sage: e(M_karan)
ELSSGVYVUTEM
sage:
sage: # Lalit Gour
sage: M_Lalit = S("LALITGOUR")
sage: e(M_Lalit)
JIKCKNKRA
```

```
sage:
sage: E = TranspositionCryptosystem(S, 3)
sage: K = E.random_key()
sage: Ki = E.inverse_key(K)
sage: e = E(K)
sage: d = E(Ki)
sage:
sage:
sage: # Vedant
sage: e(M_ved)
EDVNTA
sage:
sage: # Karan
sage: e(M_karan)
ARKNKAMBUARH
sage:
sage: # Lalit Gour
sage: e(M_Lalit)
ALLTGIURO
sage:
```

```
sage:
sage: # Vigenere
sage: E = VigenereCryptosystem(S,3)
sage: K = E.random_key()
sage: L = E.inverse_key(K)
sage: e = E(K)
sage: c = E(L)
sage:
sage:
sage: # Vedant
sage: e(M_ved)
GEELNU
sage:
sage: # Karan
sage: e(M_karan)
VASLNLFMCSAS
sage:
sage: # Lalit Gour
sage: e(M_Lalit)
WAMTTHZUS
sage:
```

The Vigenere cipher, a polyalphabetic substitution cipher, has historically been considered one of the strongest encryption methods. The cipher employs a keyword that repeats itself to shift each character of the plaintext. Despite its apparent complexity, the Vigenere cipher can be broken using several cryptanalytic techniques.

In this case study i will focus on a sophisticated method for breaking the Vigenère cipher: Kasiski examination.

So let first understand how vigenere cipher works: The Vigenere cipher encrypts plaintext by shifting each letter according to the corresponding letter of a repeating keyword. If the keyword is "LEMON" and the plaintext is "ATTACKATDAWN," the cipher aligns the keyword with the plaintext and shifts each letter accordingly.

Plaintext: ATTACKATDAWN
Keyword: LEMONLEMONLE
Ciphertext: LXFOPVEFRNHR

The shift for each letter is determined by the position of the corresponding keyword letter in the alphabet (A=0, B=1, ..., Z=25).

Cryptanalysis Strategy: Kasiski Examination

Kasiski Examination involves identifying repeated sequences of characters in the ciphertext and analyzing the distances between them. The idea is that these repeated sequences likely result from the repetition of the same plaintext under the same part of the key. By finding the greatest common divisor (GCD) of these distances, we can estimate the length of the keyword.

Once the keyword length is determined, the ciphertext can be treated as several Caesar ciphers, each of which can be solved using frequency analysis.

Steps Involved in Kasiski Examination:

- Identify Repeated Sequences: Search for repeated sequences of characters in the ciphertext.
- Calculate Distances: Determine the distance between the start positions of each repeated sequence.
- Determine Keyword Length: Compute the GCD of these distances to estimate the keyword length.
- Frequency Analysis: Once the keyword length is identified, split the ciphertext into columns based on this length and perform frequency analysis on each column to deduce the keyword.

The Kasiski examination effectively reduces the problem of breaking the Vigenere cipher to solving multiple Caesar ciphers.