1. Breaking Shift Cipher and Mono-alphabetic Substitution cipher using frequency analysis method. Write here about shift cipher, mono-alphabetic substitution cipher, cipher

SHIFT CIPHER:

- A shift cipher, also known as the Caesar cipher, is one of the simplest and oldest forms of encryption techniques. It is a substitution cipher where each letter in the plaintext is shifted a certain number of positions down the alphabet. This number is called the "key" or "shift value."
- For example, with a shift value of 3, the letter "A" would be encrypted to "D," "B" to "E," and so on. The process wraps around the alphabet, so "X" would be encrypted to "A," "Y" to "B," and "Z" to "C."
- The Caesar cipher is easy to break because it has only 25 possible keys. An attacker can quickly try all shifts to decode the message, making it exposed to simple attacks.
- Shift Cipher Steps:
- From part 1 take cipher text put on cipher text in part 3 then click on decrypt with changing key from shift dropdown now take suitable plain text put on the part 4 with key which is same as shift number and get answer correct or not correct

Mono-alphabetic Substitution Cipher:

- A Monoalphabetic Substitution Cipher is a type of substitution cipher where each letter of the plaintext is replaced by a corresponding letter in the ciphertext consistently throughout the entire message. In this cipher, a fixed substitution table is used, and each letter in the plaintext is replaced by the corresponding letter in the table.
- For example, if we use a monoalphabetic substitution cipher with the following table:
  Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  Ciphertext: XYZABCDEFGHIJKLMNOPQRSTUVW
- Then the word "HELLO" would be encrypted as "EBIIL" using the substitution table above. a monoalphabetic substitution cipher can be broken by a brute force attack. A brute force attack is an attempt to systematically try all possible keys until the correct one is found. In the case of a monoalphabetic substitution cipher, the key is the substitution table, which maps each letter of the alphabet to a corresponding letter in the ciphertext.
- The reason why a brute force attack can be effective against a monoalphabetic substitution cipher is that there are only 26! (26 factorial) possible keys. Since each letter of the alphabet can be substituted with any other letter exactly once, the total number of possible keys is: 26! = 26 × 25 × 24 × ... × 3 × 2 × 1 ≈ 4.03 × 10^26 With sufficient computing power, a brute force attack can quickly test all possible keys and identify the correct one.
- Frequency analysis can aid in breaking a monoalphabetic substitution cipher. Since the same plaintext letters are consistently replaced by the same ciphertext letters, patterns emerge in the frequency distribution of letters in the ciphertext. For example, the most frequent letter in the ciphertext is likely to represent the letter 'e' in the plaintext, which is the most common letter in the English language.
- Mono-alphabetic Substitution Cipher Steps:

Cipher	d	k	x	y	v	r	h	u	w	e	c	q	g	t	n	p	s	o	f	i	b	l	m
Plain	C	h	a	p	t	e	r	l	i	o	b	d	w	n	s	g	v	k	m	u	y	f	z

Solution key: xodqrlpkwzoufteyahnvisgjbm

2. Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenere cipher.
    - Vigenere Cipher Steps:
      The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. It uses a keyword (or keyphrase) to determine the shift value for each letter in the plaintext. The keyword is repeated as necessary to match the length of the plaintext. In the Vigenère cipher, you use a keyword (or keyphrase) to determine the shift value for each letter in your plaintext. First, choose a keyword that you'll repeat to match the length of your plaintext.
      For example, let's say your keyword is "KEY" and your plaintext is "HELLO" (all in uppercase).
      Keyword: "KEYKEY" (repeating the keyword to match the length of the plaintext).
      Plaintext: "HELLO." Next, refer to the Vigenère Table (or Vigenère Square).
      Encrypt your plaintext:
        ● Match each letter of your plaintext with the corresponding letter of your keyword (H -> K, E -> E, L -> Y, L -> K, O -> E).
        ● Find the corresponding letter in the Vigenère table at the intersection of the row and column of the matching letters.
        ● Your encrypted ciphertext is "KYKYE."
    - Playfair Cipher Steps:
      The Playfair cipher is a digraphic substitution cipher used to encrypt plaintext. It operates on pairs of letters (digraphs) instead of individual letters, making it more secure than simple substitution ciphers. The cipher uses a 5x5 matrix (Playfair square) of letters, typically excluding "J," to create the encryption key.
      In the Playfair cipher example, the keyword "KEYWORD" is used to generate the Playfair square.
      The plaintext "HELLO WORLD" is preprocessed into digraphs ("HE LX LO WO RL DX"). Applying encryption rules, the digraphs are encrypted: "HE" becomes "EK," "LX" becomes "RC," "LO" becomes "OD," and "WO" becomes "BM." The final ciphertext is "EKRCOMEDY." To decrypt, both sender and receiver must use the same Playfair square with the shared keyword to reverse the process and retrieve the original plaintext "HELLOWORLD." The cipher's digraphic approach enhances security compared to simple substitution ciphers, making it a valuable historical
      encryption technique.

3. To study Block cipher modes of operation using Advanced Encryption Standard (AES).
   MODES OF OPERATION:
   Refer shreya pdf
    - ECB Mode (Electronic Codebook Mode) Steps:
      Part 2 get plain text, key, from part 4 get cipher text and put in part 5
    - CBC Mode (Cipher Block Chaining Mode) Steps:

Part 2 get plain text and key and iv , in part 3 whatever xor get put in part 4 plain text to get cipher text and put that in answer (all 5 together)

- OFB Mode (Output Feedback Mode) Steps:
  Same as cbc

4. RSA
   Refer shreya pdf for theory
   - RSA Steps: write text then in rsa private key section mai generate click karne then click on encrypt button then click decrypt button
   - Digital system Steps:
     Hash joh bhi aayege input to rsa mai daalne public key mai 512 e=3 karne