**Classical Cipher**

**1. Caesar Cipher**

Encryption:

* Choose a shift value (key) from 1 to 25.
* For each letter in the plaintext, shift it by the chosen value down the alphabet.

Decryption:

Reverse the shift operation on the ciphertext using the same key.

Brute Force Attack:

* Try all possible shift values from 1 to 25.
* Analyze the output using frequency analysis or other heuristic techniques to find the most likely plaintext.

**2. Monoalphabetic Substitution Cipher**

Encryption:

* Choose a random one-to-one mapping of the alphabet to another set of letters.
* Replace each letter in the plaintext with the corresponding letter from the mapping.

Decryption:

Reverse the substitution using the inverse mapping.

Brute Force Attack:

* Brute force is not practical due to 26! possible key combinations.
* Use frequency analysis to find the most likely substitution mapping.

**3. Vigenère Cipher**

Encryption:

* Choose a keyword.
* Repeat the keyword until it matches the length of the plaintext.
* Shift each plaintext letter by the corresponding keyword letter's position in the alphabet.

Decryption:

1. Reverse the shift operation on the ciphertext using the corresponding keyword letter's position in the alphabet.

Brute Force Attack:

* Try different keyword lengths.
* Apply frequency analysis on the resulting Caesar ciphers for each keyword length.
* Determine the most likely keyword length based on the analysis.
* Perform frequency analysis on each Caesar cipher to recover the keyword.