Pre Lab:-

1. What is the Affine cipher, and how does it differ from the Caesar cipher?
The Affine cipher is a substitution cipher that uses a linear function for encryption, combining multiplication and addition, whereas the Caesar cipher only shifts characters by a fixed number.

2. Explain the mathematical formula used in the encryption and decryption process of the Affine cipher.
Encryption: $E(x)=(ax+b) \bmod m$
Decryption: $D(y)=a-1(y-b) \bmod m$, where a and $a-1$ are keys and the modular inverse, respectively.

3. How does the Affine cipher achieve encryption and decryption using modular arithmetic?
Encryption and decryption use modular arithmetic to ensure that the transformed values wrap around within the alphabet range, keeping the results within a defined set of characters.

4. What are the requirements for selecting valid keys in the Affine cipher?
The key A must be coprime with the size of the alphabet to ensure a valid modular inverse exists, while B can be any integer.

5. Discuss the significance of the keys 'a' and 'b' in the Affine cipher and how they affect the encryption process.
Key A controls the multiplicative shift, affecting the cipher's complexity and the ability to invert the transformation, while key B determines the additive shift, altering the initial position of the characters.

VIVA:-

1. How does the choice of alphabet size 'm' affect the security and complexity of the Affine cipher?
The alphabet size mmm impacts the number of possible key pairs and valid transformations. A larger mmm increases complexity and security, but if too small, it makes brute-force attacks easier.

2. Describe the process of encrypting and decrypting a message using the Affine cipher with a specific set of keys.
For encryption, apply the formula $E(x)=(ax+b) \bmod m$. For decryption, use $D(y)=a-1(y-b) \bmod m$, where a, $a-1$, and b are the keys, and each letter corresponds to a number between 0 and $m-1$.

3. What are the advantages of using the Affine cipher over simpler substitution ciphers like the Caesar cipher?
The Affine cipher is more complex, combining both multiplicative and additive shifts, which increases the number of possible keys, making it harder to break compared to the single-shift Caesar cipher.

4. Discuss the vulnerabilities of the Affine cipher and potential attacks to break the encryption.
Affine cipher is vulnerable to frequency analysis since it's a simple substitution cipher. A chosen-plaintext or known-plaintext attack can also be used to determine the keys by solving linear equations.

5. Compare the security of the Affine cipher with other classical and modern encryption techniques.
Compared to classical ciphers like the Caesar cipher, the Affine cipher offers more security but remains weak against modern attacks. Modern encryption algorithms, like AES, offer vastly superior security through complex transformations and key management.