Pre-Lab:

1.**What is Public-key cryptography (Asymmetric cryptography)?**

A cryptographic system where a pair of keys—one public and one private—are used; the public key encrypts data, and only the private key can decrypt it.

2.**What is Symmetric key cryptography (Private key cryptography)?**

A cryptographic system where the same key is used for both encryption and decryption, requiring the key to be kept secret between the communicating parties.

3.**What is an Affine cipher?**

A type of substitution cipher that combines multiplication and addition to encrypt each letter of the plaintext, using a mathematical formula.

4.**What is a Caesar cipher?**

A substitution cipher where each letter in the plaintext is shifted a fixed number of positions down or up the alphabet.

5.**What is the Miller–Rabin primality test?**

A probabilistic algorithm used to determine if a number is likely to be prime, providing faster results than deterministic methods for large numbers.

6.**What is the Euclidean Algorithm for finding GCD(A, B)?**

An efficient method to find the greatest common divisor (GCD) of two numbers by repeatedly applying the division algorithm.

7.**What is the Rabin Cryptosystem?**

An asymmetric encryption algorithm based on the difficulty of factorizing the product of two large prime numbers, similar in principle to RSA but with different decryption complexities.

VIVA:

1.**What is an Affine cipher?**

A type of substitution cipher that combines multiplication and addition to encrypt each letter of the plaintext, using a mathematical formula.

2.**What is a Caesar cipher?**

A substitution cipher where each letter in the plaintext is shifted a fixed number of positions down or up the alphabet.

3.**What is the Miller–Rabin primality test?**

A probabilistic algorithm used to determine if a number is likely to be prime, providing faster results than deterministic methods for large numbers.

4.**What is the Rabin Cryptosystem?**

An asymmetric encryption algorithm based on the difficulty of factorizing the product of two large prime numbers, similar in principle to RSA but with different decryption complexities.

5.**Explain the Euclidean Algorithm.**

An efficient method to find the greatest common divisor (GCD) of two numbers by repeatedly applying the division algorithm until the remainder is zero.