Pre-Lab:

1.What is the Miller-Rabin Primality Test?

The Miller-Rabin Primality Test is a probabilistic algorithm used to determine if a number nnn is prime. It expresses n−1n-1n−1 as 2s×d2^s \times d2s×d and tests whether randomly chosen bases aaa satisfy conditions that would prove nnn is composite. If nnn passes several rounds of testing, it is likely prime with a high probability, although there is a small chance of error.

2.How does RSA Encryption work with a 1024-bit Key?

RSA encryption uses a public key consisting of a 1024-bit modulus n and a public exponent e (often 65537). To encrypt a message m, the algorithm calculates $c=m^e \bmod n$, producing the ciphertext c. The 1024-bit key size ensures the encryption's strength, making it difficult to break through brute-force methods, providing strong security for sensitive communications.

3.How does RSA Decryption work with a 1024-bit Key?

RSA decryption uses the private key, which includes the 1024-bit modulus n and a private exponent d. To decrypt a ciphertext c, the algorithm computes $m=c^d \bmod n$, retrieving the original message m. The security of RSA decryption relies on the computational difficulty of factoring the large modulus n, which protects the private key and ensures that only the key holder can decrypt the message.

VIVA:

1.**How to Encrypt with a 1028-bit Key:**

To encrypt using a 1028-bit RSA key, use the public key consisting of a 1028-bit modulus n and a public exponent e. Compute the ciphertext c as $c=m^e \bmod n$, where m is the plaintext message.

2.**How to Decrypt with a 1028-bit Key:**

To decrypt using a 1028-bit RSA key, use the private key with the same 1028-bit modulus n and a private exponent d. Compute the plaintext mmm as $m=c^d \bmod n$, where c is the ciphertext.

3.**Advantages of RSA Algorithm:**

RSA provides strong security based on the difficulty of factoring large integers, allows for secure key exchange and digital signatures, and is widely supported and understood in cryptographic systems.

4.**Disadvantages of RSA Algorithm:**RSA is computationally intensive, especially with large keys, and can be slower than symmetric key algorithms for encrypting large amounts of data. It also requires secure key management to prevent unauthorized access.

5.**Explain RSA with the Use of Blockchain:**

RSA can be used in blockchain systems for securing transactions and verifying identities. For example, RSA can be employed to sign transaction data, ensuring its authenticity and integrity, and enabling secure communication between nodes in the blockchain network.