Prime numbers play a *critical role in modern encryption systems, particularly in public-key cryptography, where they form the foundation of widely used encryption algorithms such as **RSA (Rivest-Shamir-Adleman)*.Their importance lies in their mathematical properties, especially their behavior in modular arithmetic and their difficulty to factorize when part of large composite numbers.RSA Encryption: The Role of Prime Numbers* In the RSA encryption algorithm, the security of the system is based on the difficulty of factoring large composite numbers into their prime factors.- The security of this system relies on the fact that, while multiplying \(p\) and \(q\) to get \(n\) is easy, factoring \(n\) back into \(p\) and \(q\) is computationally infeasible when \(p\) and \(q\) are sufficiently large (e.g., 2048-bit primes).*Encryption and Decryption*: - Messages are encrypted using the public key and can only be decrypted using the private key.This \(n\) is used as the modulus in encryption and decryption.- A public key is created, which includes \(n\) and another number, \(e\), that satisfies certain mathematical conditions.The private key allows decryption of messages encrypted with the public key.Here's an overview of the process: 1.*Generating Keys Using Prime Numbers*: - Two large prime numbers, \(p\) and \(q\), are chosen.- Their product, \(n = p \times q\), is calculated.- A private key is derived using \(p\), \(q\), and \(e\).Here's how they are used: --- ### *1.2.--- ### *2.