**AMRUTHESH**

**241059041**

**CRYPTOLOGY**

**M.E – CYBER SECURITY**

**Introduction**

RSA (Rivest-Shamir-Adleman) is one of the most influential algorithms in the history of cryptography. Developed in 1977, RSA introduced the concept of public-key cryptography, which revolutionized data security.

**1. RSA Algorithm Overview**

**Principle:** RSA is an asymmetric encryption algorithm that uses a pair of keys: a public key for encryption and a private key for decryption.

**Key Generation:**

1. **Select Two Prime Numbers:** Choose two large prime numbers, ppp and qqq.
2. **Compute the Modulus:** n=p×qn = p \times qn=p×q. This modulus is used in both the public and private keys.
3. **Calculate the Totient Function:** ϕ(n)=(p−1)×(q−1)\phi(n) = (p-1) \times (q-1)ϕ(n)=(p−1)×(q−1).
4. **Choose the Public Exponent:** Select an integer eee such that 1<e<ϕ(n)1 < e < \phi(n)1<e<ϕ(n) and eee is coprime with ϕ(n)\phi(n)ϕ(n).
5. **Determine the Private Exponent:** Calculate ddd, the modular multiplicative inverse of eee modulo ϕ(n)\phi(n)ϕ(n).

**Encryption and Decryption:**

* **Encryption:** ciphertext=plaintextemod  n\text{ciphertext} = \text{plaintext}^e \mod nciphertext=plaintextemodn
* **Decryption:** plaintext=ciphertextdmod  n\text{plaintext} = \text{ciphertext}^d \mod nplaintext=ciphertextdmodn

**2. Impact on Public-Key Cryptography**

**Security Basis:**

* **Factorization Problem:** The security of RSA relies on the difficulty of factoring the product of two large prime numbers. While it is easy to multiply two primes, factoring their product into the original primes is computationally hard.

**Key Distribution:**

* **Public and Private Keys:** RSA allows for secure key distribution. The public key can be openly shared, while the private key remains confidential, enabling secure communication without the need for a pre-shared secret key.

**Digital Signatures:**

* **Authentication and Integrity:** RSA can also be used to create digital signatures, which provide authentication and integrity for digital messages. The sender signs the message with their private key, and the recipient verifies the signature using the sender’s public key.

**3. Practical Applications**

**Secure Communication:**

* **TLS/SSL:** RSA is widely used in protocols like TLS/SSL to secure web communications. It ensures that data exchanged between clients and servers is encrypted and protected from eavesdropping.

**Public-Key Infrastructure (PKI):**

* **Certification Authorities:** RSA is integral to PKI, which relies on certificate authorities (CAs) to issue and manage digital certificates. These certificates verify the identity of entities and facilitate secure communications.

**4. Limitations and Advances**

**Key Length and Security:**

* **Key Size:** RSA’s security is influenced by key length. Longer keys provide better security but also require more computational resources. The recommended minimum key size is 2048 bits for adequate security.

**Post-Quantum Cryptography:**

* **Quantum Threats:** RSA’s security may be compromised by quantum computers, which can solve the factorization problem efficiently using algorithms like Shor’s algorithm. Research into post-quantum cryptography is ongoing to develop new algorithms resistant to quantum attacks.

**Conclusion**

RSA’s introduction of public-key cryptography marked a significant advancement in securing digital communications. Its principles continue to underpin modern cryptographic practices, despite emerging challenges and ongoing developments in the field.