RSA In Cryptography:

RSA (Rivest-Shamir-Adleman) is a widely-used public-key encryption algorithm in cryptography.

In RSA encryption, each user has a pair of keys: a public key and a private key. The public key can be freely distributed and is used for encryption, while the private key is kept secret and is used for decryption. The security of RSA relies on the difficulty of factoring large composite numbers into their prime factors.

1. **Key Generation**:

   - Choose two large prime numbers, p and q.
   - Compute their product, $n = p \times q$. n is part of both the public and private keys.
   - Compute $\phi(n) = (p-1) \times (q-1)$, where ϕ is Euler's totient function.
   - Choose an integer e such that $1 < e < \phi(n)$ and e is coprime with $\phi(n)$. e becomes the public exponent.
   - Compute the modular multiplicative inverse d of e modulo $\phi(n)$, i.e., $d \times e \equiv 1 \pmod{\phi(n)}$. d becomes the private exponent.

2. **Encryption**:

   - Convert the plaintext message M into an integer m such that $0 \leq m < n$.
   - Encrypt m using the public key: $c = m^e \bmod n$. The resulting ciphertext c is sent to the recipient.

3. **Decryption**:

   - The recipient uses their private key to decrypt the ciphertext: $m = c^d \bmod n$.

RSA encryption provides confidentiality and authentication. It ensures that only the intended recipient with the corresponding private key can decrypt the ciphertext to obtain the original plaintext. RSA is widely used in various applications, including secure communication protocols (like HTTPS), digital signatures, secure email, and secure authentication mechanisms.