RSA Algorithm

The RSA algorithm is a widely used public-key encryption algorithm named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on the mathematical concepts of prime factorization and modular arithmetic.

The algorithm for RSA is as follows:

1. Select 2 prime numbers, preferably large, p and q.
2. Calculate n = p\*q.
3. Calculate phi(n) = (p-1)\*(q-1)
4. Choose a value of e such that 1<e<phi(n) and gcd(phi(n), e) = 1.
5. Calculate d such that d = (e^-1) mod phi(n).

Here the public key is {e, n} and private key is {d, n}. If M is the plain text then the cipher text C = (M^e) mod n. This is how data is encrypted in RSA algorithm. Similarly, for decryption, the plain text M = (C^d) mod n.

**Example:** Let p=3 and q=11 (both are prime numbers).

* Now, n = p\*q = 3\*11 = 33
* phi(n) = (p-1)\*(q-1) = (3-1)\*(11-1) = 2\*10 = 20
* Value of e can be 7 since 1<7<20 and gcd(20, 7) = 1.
* Calculating d = 7^-1 mod 20 = 3.
* Therefore, public key = {7, 33} and private key = {3, 33}.

Suppose our message is M=31. You can encrypt and decrypt it using the RSA algorithm as follows:

**Encryption:** C = (M^e) mod n = 31^7 mod 33 = 4

**Decryption:** M = (C^d) mod n = 4^3 mod 33 = 31

Since we got the original message that is plain text back after decryption, we can say that the algorithm worked correctly.