RSA Algorithm

It was developed by Rivest, Shamir and Adleman. This algorithm makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2 (n)$; in practice, the block size is k-bits, where $2^k < n < 2^{k+1}$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

$$C = M^e \bmod n$$

$$M = C^{d \bmod} n = (M^e \bmod n) \bmod n$$

$$= (M^e)^d \bmod n$$

$$= M^{ed} \bmod n$$

Both the sender and receiver know the value of n. the sender knows the value of e and only the receiver knows the value of d. thus, this is a public key encryption algorithm with a public key of KU = {e, n} and a private key of KR = {d, n}. For this algorithm to be satisfactory for public key encryption, the following requirements must be met:

- It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M<n$.
- It is relatively easy to calculate M^e and C^d for all values of $M<n$.
- It is infeasible to determine d given e and n.

Let us focus on the first requirement. We need to find the relationship of the form:

$$M^{ed} = M \bmod n$$

A corollary to Euler's theorem fits the bill: Given two prime numbers p and q and two integers, n and m, such that $n=pq$ and $0<m<n$, and arbitrary integer k, the following relationship holds

DIFFIE-HELLMAN KEY EXCHANGE

The purpose of the algorithm is to enable two users to exchange a key securely that can then be used for subsequent encryption of messages.

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. First, we define a primitive root of a prime number p as one whose power generate all the integers from 1 to (p-1) i.e., if ‘a’ is a primitive root of a prime number p, then the numbers

$$a \bmod p,\ a^2 \bmod p,\ \ldots\ a^{p-1} \bmod p$$

are distinct and consists of integers from 1 to (p-1) in some permutation. For any integer ‘b’ and a primitive root ‘a’ of a prime number ‘p’, we can find a unique exponent ‘i’ such that

$$b \equiv a^i \bmod p \text{ where } 0 \leq i \leq (p-1)$$

The exponent ‘i’ is referred to as discrete logarithm. With this background, we can define Diffie Hellman key exchange as follows:

There are publicly known numbers: a prime number ‘q’ and an integer α that is primitive root of q. suppose users A and B wish to exchange a key. User A selects a random integer $X_A < q$ and computes $Y_A = \alpha^{XA} \bmod q$. Similarly, user B independently selects a random integer $X_B < q$ and computes $Y_B = \alpha^{XB} \bmod q$. Each side keeps the X value private and makes the Y value available publicly to the other side. User A computes the key as

$$K = (Y_B)^{XA} \bmod q \text{ and}$$

User B computes the key as

$$K = (Y_A)^{XB} \bmod q$$

These two calculations produce identical results.