RSA algorithm

* Rivest Shamir Adleman developed in 1978
* It is an asymmetric encryption algorithm
* Two keys ie public and private key concept is used
* Public key → known to all user's in Network
* Private key → Kept secret, not sharable to all
* Public key used for encryption and private key for decryption
* RSA Algorithm is a block cipher

Key generation by Alice

① Select p, q // p and q both prime $p \neq q$

② calculate $n = p \times q$

③ calculate $\phi(n) = (p-1)(q-1)$

④ select integer e (Public key)

$$\gcd(\phi(n), e) = 1 \; ; \quad 1 < e < \phi(n)$$

⑤ calculate d (Private key)

$$d \equiv e^{-1} \pmod{\phi(n)}$$

$$ed = 1 \bmod \phi(n)$$

$$ed \bmod \phi(n) = 1$$

⑥ Public key $PU = \{e, n\}$

⑦ private key $PR = \{d, n\}$

Encryption by Bob with Alice's public key

Plain Text : $M < n$

Cipher text : $\boxed{C = M^e \bmod n}$

Decryption by Alice with Alice Public key

Cipher text : C

plain Text : $\boxed{M = C^d \bmod n}$

eg:

$P = 3, q = 11, e = 7, M = 31$

$n = P * q = 3 \times 11 = 33$

$\phi(n) = (P-1) \times (q-1)$

$= 2 \times 10 = 20$

So let $e = 7$ as $1 < 7 < 20$ and $\gcd(7, 20) = 1$

Calculate d

$d \equiv e^{-1} \bmod \phi(n)$

$d e \bmod \phi(n) = 1$

$d \times 7 \bmod 20 = 1$ $\quad d = 3$

$21 \bmod 20 = 1$

so $d = 3$

Public key $= \{e, n\} = \{7, 33\}$

Private key $= \{d, n\} = \{3, 33\}$

Encryption

$M = 31$

$C = M^e \bmod n$

$C = 31^7 \bmod 33$

$\boxed{C = 4}$

decryption

$M = C^d \bmod n$

$= 4^3 \bmod 33$

$\boxed{M = 31}$

— x —

<u>eg 2</u>

Perform encryption and decryption using the RSA algorithm

$p = 3,\ q = 7,\ e = 5,\ M = 10$

Key generation

given $p = 3,\ q = 7$

$n = p \times q = 3 \times 7 = 21$

$\phi(n) = (p-1) \times (q-1)$

$= 2 \times 6 = 12$

$e = 5$; $1 < 5 < 12$ and $\gcd(5, 12) = 1$

Calculate

$d \equiv e^{-1} \bmod \phi(n)$

$de \bmod \phi(n) = 1$

$d \times 5 \bmod 12 = 1$

ie $d = 5$

Public key = $\{5, 21\}$

Private key = $\{5, 21\}$

Encryption

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

$M = 10$

$$C = 10^5 \bmod 21$$

$$C = 19$$

Decryption

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

$$M = 19^5 \bmod 21$$

$$M = 10$$

— x —

eg3

Perform encryption and decryption using RSA algorith
$p = 17$, $q = 11$, $e = 7$, $M = 88$

eg4

In a public key system using RSA you intercept the cipher text $C = 12$ sent to a user use public key =
$n = 77$ find the plain Text M

Step 1:

compute d

$n = 77$

$$\boxed{\begin{matrix} P = 7 \\ q = 11 \end{matrix}}$$

$n = p \times q = 7 \times 11$

$\phi(n) = (P-1)(q-1) = 6 \times 10 = 60$

Find d

$d \equiv e^{-1} \bmod \phi(n)$

$d \times e \bmod \phi(n) = 1$

$d \times 7 \bmod 60 = 1$

$\boxed{d = 43}$

Find M (Plain Text)

$M = c^d \bmod n$

$M = 12^{43} \bmod 77$

$\boxed{M = 31}$

—x—

eg 5

In an RSA system, the public key of a given user ie $e = 7, n = 187$ Determine the Private key of this user?

Diffie hellman Key exchange

→ Key exchange algorithm, not an encryption algorithm.

→ used to exchange secret keys between two users

→ use ~~sy~~ asymmetric encryption to exchange the secret key.

→ There are 2 publicly known numbers; prime no's q and an integer α that is a primitive root of q.

Algorithm

1. Consider a prime number q
2. Select α such that it must be the primitive root of q and α < q

a is a primitive root of q if

$a^1 \bmod q$

$a^2 \bmod q$

$a^3 \bmod q$

⋮

$a^{q-1} \bmod q$

gives results {1, 2, 3 ... q-1}

Values should not be repeated and we should have all values in the output set from 1 to q-1 eg $q = 7$

$\alpha < q$ It is a primitive root

take 3

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

$3^6 \bmod 7 = 1$

$5^1 \bmod 7 = 5$

$5^2 \bmod 7 = 4$

$5^3 \bmod 7 = 6$

$5^4 \bmod 7 = 2$

$5^5 \bmod 7 = 3$

$5^6 \bmod 7 = 1$

primitive root 3 or 5

take any of the primitive root 3 or 5

take any of the primitive element

α and q → global public element

Key generation of user A

Assume private key $X_A = 3$ $\quad X_A < q$

X – private key of user

Y – public key of user

Calulate

$$Y_A = \alpha^{X_A} \bmod q$$

$$Y_A = \alpha^{X_A} \bmod q$$

$$Y_A = 5^3 \bmod 7$$

$$\boxed{Y_A = 7}$$

Key generation of user B

assume X_B

$$Y_B = \alpha^{X_B} \bmod q$$

$$Y_B = 5^4 \bmod 7 \quad \boxed{Y_B = 2}$$

Calculate Secret key

To calculate the secret key both sender and receiver will use public key

$K_1 = (YB)^{XA} \bmod q$ $\quad$ $K_2 = (YA)^{XB} \bmod q$

YA & $YB \rightarrow$ Public keys

$K_1 = K_2$ then we say exchange is successful

Secret key calculation by user A

$K_1 = (YB)^{XA} \bmod q$

$= 2^3 \bmod 7$

$\boxed{K_1 = 1}$

Secret key calculation by user B

$K_2 = (YA)^{XB} \bmod q$

$= 6^4 \bmod q$

$\boxed{K_2 = 1}$ $\quad$ $\boxed{K_1 = K_2}$ Key exchange successful.

—x—