RSA

Formulas

Select p, q	p and q both prime, $p \neq q$
$n = p \times q$	
$\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d = e^{-1}(mod\ \phi(n))$
Public Key	$PU = \{e, n\}$
Private Key	$PR = \{d, n\}$
Ciphertext, C	$C = M^e\ mod\ n$
Plaintext, M	$M = C^d\ mod\ n$

Example # 1

Given p = 7, q = 19, find e.

Solution:

$\gcd(\phi(n), e) = 1$

$\phi(n) = (p - 1) \times (q - 1) = 6 \times 18 = 108$

$\gcd(108, e) = 1$

Let's try value of e = 2, 3, 4, 5

$\gcd(108, 2)$

Divisors of 108 : 1, 2, 3, 4, 6, 12, 18, 108

Divisors of 2 : 1, 2

The greatest common divisor: 2, so not qualified.

Gcd(108, 5)

Divisors of 108 : 1, 2, 3, 4, 6, 12, 18, 108

Divisors of 5 : 1, 5

The greatest common divisor: 1, so qualified.

∴ e = 5

Example # 2

Using the RSA algorithm with p = 47, q = 53, and e = 19.

a. Calculate the decryption key d.

b. Encrypt the message M = 03.

Solution

Given, p = 47, q = 53, and e = 19

a. Calculating the decryption key d

$d = e^{-1}(mod\ \phi(n))$

$\phi(n) = (p\text{-}1) \times (q\text{-}1) = 46 \times 52 = 2392$

$d = 19^{-1}(mod\ 2392)$

Now, using the formula,

$$d = \frac{(k\ x\ \phi(n) + 1)}{e}$$

where k = 1, 2, 3, … until an integer value for d can be found

$$d = \frac{(10\ x\ 2392 + 1)}{19} = \ 1259\ [\text{Here, k} = 10 \text{ provides an integer value for d}]$$

$\therefore d = 19^{-1}(mod\ 2392) = \boldsymbol{1259}$

b. Encrypt the message M = 03

$C = M^e\ mod\ n$

$n = p \times q = 47 \times 53 = 2491$

$C = 3^{19}\ mod\ 2491 =>$

$$\frac{3^{19}}{2491} = 466584.29024488$$

2491 x (466584.29024488 – 466584) = 723

$\therefore C = 3^{19}\ mod\ 2491 = \boldsymbol{723}$

Example # 3

If the RSA public key of a user is (e = 5, n = 1343), attempt to deduce the value of the private key d (i.e. break the key).

Solution

Step 1:

Public key PU = {e, n} = {5, 1343}

$n = p \, x \, q$

Let's try,

$p = \frac{n}{q}$ [for q = 2, 3, 5, 7,11,13,17 … until an integer prime number for q is found]

$$p = \frac{1343}{2} = 671.50 \text{ [Not good]}$$
$$p = \frac{1343}{3} = 447.66 \text{ [Not good]}$$
$$p = \frac{1343}{5} = 268.60 \text{ [Not good]}$$
$$p = \frac{1343}{7} = 191.85 \text{ [Not good]}$$
$$p = \frac{1343}{11} = 122.09 \text{ [Not good]}$$
$$p = \frac{1343}{13} = 103.30 \text{ [Not good]}$$
$$p = \frac{1343}{17} = 79 \text{ [Good choice since } p \text{ is also a prime number]}$$

Thus p, q = 79, 17

Step 2: Now let us deduce the value of the private key *d*

$d = e^{-1}(mod\ \phi(n))$

$\phi(n) = (p\text{-}1)\ x\ (q\text{-}1) = 78\ x\ 16 = 1248$

$d = 5^{-1}(mod\ 1248)$

Now, using the formula,

$$d = \frac{(k\ x\ \phi(n) + 1)}{e}$$

where k = 1, 2, 3, … until an integer value for d can be found

$$d = \frac{(1\ x\ 1248 + 1)}{5} = 249.8 \text{ [Not good]}$$
$$d = \frac{(2\ x\ 1248 + 1)}{5} = 499.4 \text{ [Not good]}$$
$$d = \frac{(3\ x\ 1248 + 1)}{5} = 749 \text{ [Good]}$$

$\therefore d = 5^{-1}(mod\ 1248) = \boldsymbol{749}$