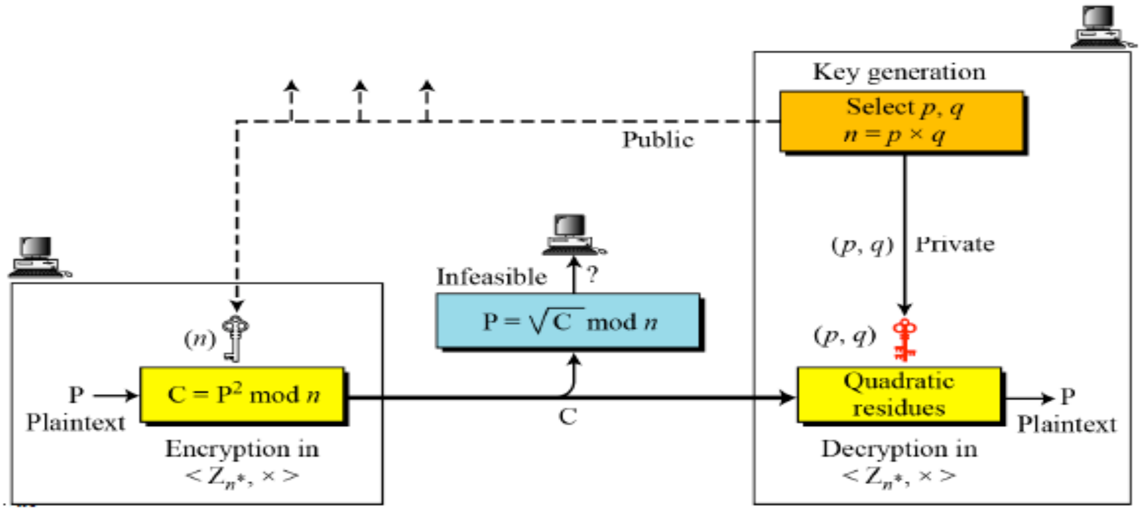
Practical Number 6

Aim: To implement Rabin Cryptosystem.

Theory: The Rabin cryptosystem, devised by M. Rabin, is a variation of the RSA cryptosystem. RSA is based on the exponentiation congruence; Rabin is based on quadratic congruence. The Rabin cryptosystem can be thought of as an RSA cryptosystem in which the value of e and d are fixed, e = 2 and d = ½. In other words, the encryption is $C \equiv P^2 \pmod{n}$ and the decryption is $P \equiv C^{1/2} \pmod{n}$.

The public key in Rabin cryptosystem is n; the private key is the tuple (p, q). Everyone can encrypt a message using n; only the receiver can decrypt the message using p and q. Decryption of the message is infeasible for the attacker because he/she does no know the values of p and q. In RSA, the receiver can keep d and n and discard p, q, and $\phi(n)$ after key generation; in Rabin cryptosystem, the receiver needs to keep p and q.



The receiver uses the key generation algorithm given below to create his public and private key.

Rabin_Key_Generation

{

Choose two large primes p and q in the form $4k + 3$ and $p \neq q$.

$n \leftarrow p \times q$

Public_key $\leftarrow n$ // To be announced publicly

Private_key $\leftarrow (q, n)$ // To be kept secret

return Public_key and Private_key

}

Although the two primes, p and q, can be in the form 4k + 1 or 4K + 3, the decryption process becomes more difficult if the first form is used. It is recommended to use the second form.

Anyone can send a message to the receiver using his public key. The encryption process is shown below

Rabin_Encryption (n, **P**) // n is the public key; P is the ciphertext from $\mathbf{Z}_n{}^*$

{

  $C \leftarrow P^2 \bmod n$ // C is the ciphertext

  return C

}

The receiver uses the algorithm given below to decrypt the received ciphertext.

Rabin_Decryption (p, q, C) // C is the ciphertext; p and q are private keys

{

  $a_1 \leftarrow +(C^{(p+1)/4}) \bmod p$
  $a_2 \leftarrow -(C^{(p+1)/4}) \bmod p$
  $b_1 \leftarrow +(C^{(q+1)/4}) \bmod q$
  $b_2 \leftarrow -(C^{(q+1)/4}) \bmod q$

  // The algorithm for the Chinese remainder algorithm is called four times.

  $P_1 \leftarrow$ Chinese_Remainder (a_1, b_1, p, q)
  $P_2 \leftarrow$ Chinese_Remainder (a_1, b_2, p, q)
  $P_3 \leftarrow$ Chinese_Remainder (a_2, b_1, p, q)
  $P_4 \leftarrow$ Chinese_Remainder (a_2, b_2, p, q)
  return P_1, P_2, P_3, and P_4

}

The decryption is based on solution of quadratic congruence. As the received ciphertext is the square of the plaintext, it is guaranteed that C has roots in $Z_n{}^*$. The Chinese remainder algorithm is used to find the four square roots.

Example: Select $p = 23$ *and* $q = 7$. *Note that both are c*ongruent to 3 mod 4.

Calculate $n = p \times q = 161$.

Announce *n publicly; keep p and q* private.

Let plaintext $P = 24$.

$C = 24^2 \bmod 162 = 93 \bmod 16$

161

The Receiver receives 93 and calculates four values:

1. $a1 = +(93^{(23+1)/4}) \bmod 23$

   $= 1 \bmod 23$

2. $a2 = -(93^{(23+1)/4}) \bmod 23$

$= 22 \bmod 23$

3. $b1 = +(93^{(7+1)/4}) \bmod 7$

   $= 4 \bmod 7$

4. $b2 = -(93^{(7+1)/4}) \bmod 7$

   $= 3 \bmod 7$

The Receiver takes four possible answers, (a1, b1), (a1, b2), (a2,b1), and (a2,b2), and uses the Chinese remainder theorem to find four possible plaintexts:

116, 24, 137, and 45

Only the second result is correct.

Rabin cryptosystem is not deterministic as it creates four possible answers.

Conclusion: The concepts of Rabin cryptosystem has been understood and successfully implemented.