Rabin Cryptosystem

1.Rabin cryptosystem is published in jan. 1979 by Michael o Rabin.

2.It is based on quadratic congruence.

3. It is Asymmetric key algo

4.Encryption is very simple

1.**Key generation:**

Step-1 :Choose two large distinct prime p,q

$P \equiv q \equiv 3 \pmod 4$

Step-2 :Let n=p*q

Public key=n

Private key=p,q

2.Encryption:-

For encryption only public key n is used

Let Zn ,the plain text space and

$C=m^2 \bmod n$,m-plain text ,C-cipher text

3. Decryption:

1.Compute under root c mod n

2. There are four square roots .out of which correct plain text is selected.

3. By adding some redundancy bits into plain text .we can recognize correct plain text.

Step:1 Using Euclidean algo find a & b

$a*p+b*q=1$

Step:2 Compute

$r=C^{(p+1)/4} \bmod p$

$s=C^{(q+1)/4} \bmod q$

$x=(a*p*s+b*q*r) \bmod n$

$y=(a*p*s-b*q*r) \bmod n$

Step 3: $m1=x$

$m2=n-x$

$m3=y$

$m4=n-y$

Example:

1. Let p=7,q=11,m=5

2. n=p*q=7*11=77(public key)

3.private key=7,11

Encryption:

$C=m^2 \bmod n$

C=52 mod 77

C=25 mod 77

C=25

Decryption:-

Step:1 **a*p+b*q=1**

-3*7+2*11=1 (a=-3,b=2)

Step-2 $r=C^{(p+1)/4} \bmod p$

R=25^2 mod 7

r=2

Step:-3 $s=C^{(q+1)/4} \bmod q$

S=25^3 mod 11

S=5

Step:4 x=(a*p*s+b*q*r) mod n

X=(-3*7*5+2*11*2) mod 77

X=-61 mod 77

X=16

Step:5 y=(a*p*s-b*q*r) mod n

y=149 mod 77

y=5

so

m1=16

m2=61

m3=5

m4=72

Security of Rabin System:

1. Secure as long as p & q large no
2. Rabin as secure as RSA.
3. It has been proven that any algorithm which decrypts a Rabin-encrypted value can be used to factor the modulus . Thus, Rabin decryption is at least as hard as the integer factorization problem, something that has not been proven for RSA. It is generally believed that there is no polynomial-time algorithm for factoring, which implies that there is no efficient algorithm for decrypting a Rabin-encrypted value without the private key .