Public Key Cryptosystem -II

Sachin Tripathi

IIT(ISM), Dhanbad

Quadratic Congurrence

In cryptography, we also need to discuss quadratic congruence that is, equations of the form

$$a_2x^2 + a_1x + a_0 \equiv 0 \pmod{n}.$$

We limit our discussion to quadratic equations in which $a_2 = 1$ and $a_1 = 0$, that is equations of the form

$$X^2 \equiv a \pmod{n}.$$

Quadratic Residues and Nonresidue

In the equation $x^2 \equiv a \pmod p$, a is called a **quadratic residue (QR)** if the equation has two solutions; a is called **quadratic nonresidue (QNR)** if the equation has no solutions. It can be proved that in $\mathbf{Z}_p{}^*$, with $p - 1$ elements, exactly $(p - 1)/2$ elements are quadratic residues and $(p - 1)/2$ are quadratic nonresidues.

Example 9.41

There are 10 elements in $\mathbf{Z}_{11}{}^*$. Exactly five of them are quadratic residues and five of them are nonresidues. In other words, $\mathbf{Z}_{11}{}^*$ is divided into two separate sets, QR and QNR, as shown in Figure 9.4.

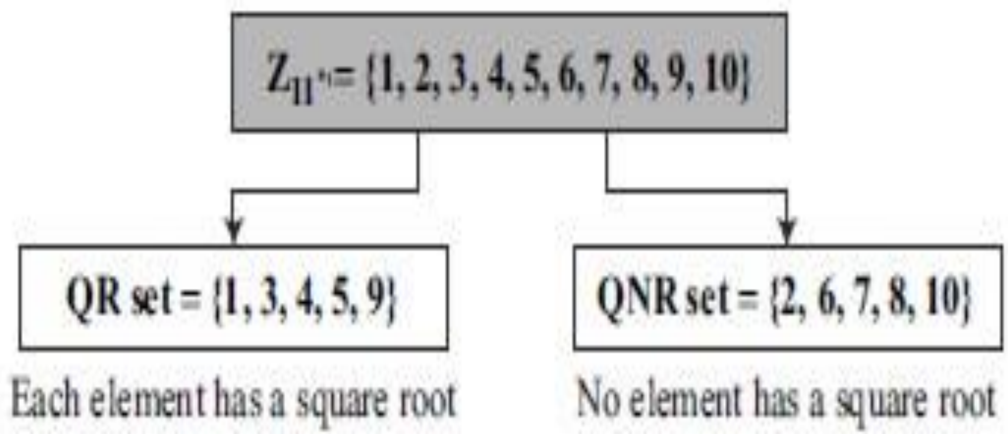
Euler's Criterion

How can we check to see if an integer is a QR modulo p? Euler's criterion gives a very specific condition:

a. If $a^{(p-1)/2} \equiv 1 \pmod p$, a is a quadratic residue modulo p.

b. If $a^{(p-1)/2} \equiv -1 \pmod p$, a is a quadratic nonresidue modulo p.

Division of $\mathbf{Z}_{11}$ elements into QRs and QNRs*



Example

To find out if 14 or 16 is a QR in $\mathbf{Z}_{23}{}^*$, we calculate:

$14^{(23-1)/2} \bmod 23 \rightarrow 14^{11} \bmod 23 \rightarrow 22 \bmod 23 \rightarrow -1 \bmod 23$	**nonresidue**
$16^{(23-1)/2} \bmod 23 \rightarrow 16^{11} \bmod 23 \rightarrow 1 \bmod 23$	**residue**

Solving Quadratic Equation Modulo a Prime

Although the Euler criterion tells us if an integer a is a QR or QNR in $\mathbf{Z}_p{}^*$, it cannot find the solution to $x^2 \equiv a \pmod p$. To find the solution to this quadratic equation, we notice that a prime can be either $p = 4k + 1$ or $p = 4k + 3$, in which k is a positive integer. The solution to a quadratic equation is very involved in the first case; it is easier in the second. We will discuss only the second case, which we will use in when we discuss Rabin cryptosystem.

Special Case: $p = 4k + 3$ If p is in the form $4k + 3$ (that is, $p \equiv 3 \bmod 4$) and a is a QR in $\mathbf{Z}_p{}^*$, then

$$x \equiv a^{(p+1)/4} \pmod p \qquad \text{and} \qquad x \equiv -a^{(p+1)/4} \pmod p$$

Example 9.43

Solve the following quadratic equations:

a. $x^2 \equiv 3 \pmod{23}$
b. $x^2 \equiv 2 \pmod{11}$
c. $x^2 \equiv 7 \pmod{19}$

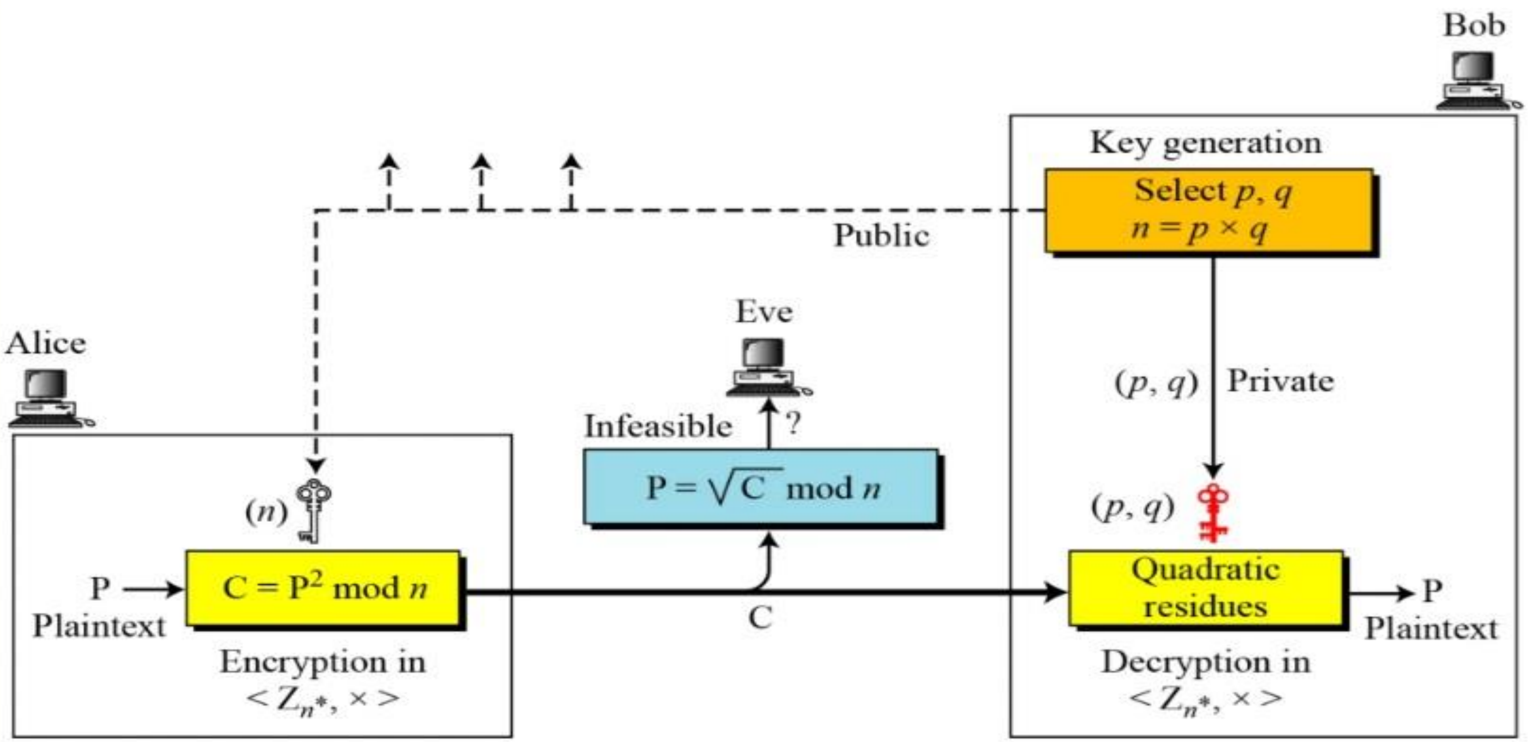
Solutions

a. In the first equation, 3 is a QR in $\mathbf{Z}_{23}$. The solution is $x \equiv \pm 16 \pmod{23}$. In other words, $\sqrt{3} \equiv \pm 16 \pmod{23}$.
b. In the second equation, 2 is a QNR in $\mathbf{Z}_{11}$. There is no solution for $\sqrt{2}$ in $\mathbf{Z}_{11}$.
c. In the third equation, 7 is a QR in $\mathbf{Z}_{19}$. The solution is $x \equiv \pm 11 \pmod{19}$. In other words, $\sqrt{7} \equiv \pm 11 \pmod{19}$.

Rabin Cryptosystem

The Rabin cryptosystem can be thought of as an RSA cryptosystem in which the value of e and d are fixed. The encryption is $C \equiv P^2 \pmod{n}$ and the decryption is $P \equiv C^{1/2} \pmod{n}$.

Rabin cryptosystem



Key Generation

Key generation for Rabin cryptosystem

```
Rabin_Key_Generation
{
    Choose two large primes p and q in the form 4k + 3 and p ≠ q.
    n ← p × q
    Public_key ← n                          // To be announced publicly
    Private_key ← (p, q)                    // To be kept secret
    return Public_key and Private_key
}
```

Encryption

```
Rabin_Encryption (n, P)        // n is the public key; P is the ciphertext from Zn*
{
    C ← P^2 mod n              // C is the ciphertext
    return C
}
```

Decryption

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

{

$a_1 \leftarrow +(\text{C}^{(p+1)/4}) \bmod p$

$a_2 \leftarrow -(\text{C}^{(p+1)/4}) \bmod p$

$b_1 \leftarrow +(\text{C}^{(q+1)/4}) \bmod q$

$b_2 \leftarrow -(\text{C}^{(q+1)/4}) \bmod q$

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

$\text{P}_1 \leftarrow$ Chinese_Remainder (a_1, b_1, p, q)

$\text{P}_2 \leftarrow$ Chinese_Remainder (a_1, b_2, p, q)

$\text{P}_3 \leftarrow$ Chinese_Remainder (a_2, b_1, p, q)

$\text{P}_4 \leftarrow$ Chinese_Remainder (a_2, b_2, p, q)

return P_1, P_2, P_3, and P_4

}

The Rabin cryptosystem is not deterministic: Decryption creates four equally probable plaintexts.

Example

Here is a very trivial example to show the idea.

1. Bob selects $p = 23$ and $q = 7$. Note that both are congruent to 3 mod 4.
2. Bob calculates $n = p \times q = 161$.
3. Bob announces n publicly; he keeps p and q private.
4. Alice wants to send the plaintext P = 24. Note that 161 and 24 are relatively prime; 24 is in $\mathbf{Z}_{161}{}^*$. She calculates $C = 24^2 = 93 \bmod 161$, and sends the ciphertext 93 to Bob.
5. Bob receives 93 and calculates four values:
   a. $a_1 = +(93^{(23+1)/4}) \bmod 23 = 1 \bmod 23$
   b. $a_2 = -(93^{(23+1)/4}) \bmod 23 = 22 \bmod 23$
   c. $b_1 = +(93^{(7+1)/4}) \bmod 7 = 4 \bmod 7$
   d. $b_2 = -(93^{(7+1)/4}) \bmod 7 = 3 \bmod 7$
6. Bob takes four possible answers, (a_1, b_1), (a_1, b_2), (a_2, b_1), and (a_2, b_2), and uses the Chinese remainder theorem to find four possible plaintexts: 116, **24**, 137, and 45 (all of them relatively prime to 161). Note that only the second answer is Alice's plaintext. Bob needs to make a decision based on the situation. Note also that all four of these answers, when squared modulo n, give the ciphertext 93 sent by Alice.

$$116^2 = 93 \bmod 161 \qquad 24^2 = 93 \bmod 161 \qquad 137^2 = 93 \bmod 161 \qquad 45^2 = 93 \bmod 161$$

Security of the Rabin System

The Rabin system is secure as long as p and q are large numbers. The complexity of the Rabin system is at the same level as factoring a large number n into its two prime factors p and q. In other words, the Rabin system is as secure as RSA.