lec 13

Rabin public-key Encryption

Key Generation Alg.

1. Generate two large random (distinct) primes p & q (almost the same size).
2. Compute $n = p * q$
3. A's public key is "n", private key is (p, q)

Algorithm of Rabin's Scheme

Encryption by B

1. Obtain A's authentic public-key "n"
2. Represent the message as an integer "m" in $\{0, 1, \dots, n-1\}$
3. Compute ciphertext $c = m^2 \pmod{n}$
4. Send the "c" to another party "A"

Decryption by "A"

1. use <u>an algorithm</u> to find four square roots m_1, m_2, m_3, m_4 of "c" (mod n).
2. the actual message "m" is one of m_1, m_2, m_3, m_4

× Dec → Computationally more expensive

× → "A" has to decide which "m_i" is the message

$\boxed{\text{Example}}$ of Rabin's public-key scheme

key gen $\begin{cases} p = 277, \quad q = 331 \longleftarrow \text{private-key of "A"} \\ n = p \cdot q = 91687 \longleftarrow \text{public-key " "} \xrightarrow{\text{send}} \text{"B"} \end{cases}$

10-bits $\longrightarrow$ $m' = 100\underbrace{111001}$ $\longrightarrow$ $m = 1001\underbrace{111001}\underbrace{111001}$ 16-bits

$\downarrow$

$m = 40569$

Enc $\left\{ \; C = m^2 \pmod n = 40569^2 \pmod{91687} = 62111 \right.$

Dec Four square roots of $c = 62111 \pmod n$

$m_1 = 69654, \quad m_2 = 22033, \quad m_3 = 40569$

$m_4 = 51118$

check $\longrightarrow$ $(m_1 = 69654)^2 \bmod 91687 \equiv 62111$

$m_1 = 1000100000000 10110$ X

$m_2 = 1010110000 10001$ X

$m_3 = 100111100 1111001$ ✓ $\longrightarrow$ actual message

$m_4 = 11000111 1010 1110$ X

$\boxed{\text{Algorithm:}}$ Finding square roots mod n & its prime factors "p" & "q"

Input: n, p, q, "a"

output: Four square roots of $a \pmod n$

1. Use $\boxed{\text{another algorithm}}$ to find two square roots "r" and "$-r$" of "a" $\pmod p$

2. Use $\boxed{\text{anothe algorithm}}$ to find two square roots "s" and "$-s$" of "a" $\pmod q$

3. Use $\boxed{\text{EE algorithm}}$ to find

$$cp + dq = 1$$

4. $$x = r\underline{dq} + s\underline{cp} \pmod n$$
$$y = r\underline{dq} - s\underline{cp} \pmod n$$

5. return $(\mp x, \mp y) \pmod n$

$\boxed{\text{Example}}$ cipher $\rightarrow a = 62111$, $p = 277$, $q = 331$ $\quad n = pq = 91687$

p: ∓ 150 $\quad q$: ∓ 144

using EE Alg. $\longrightarrow$ $\underbrace{331}_{q} \times \underbrace{118}_{d} + \underbrace{277}_{p} \times \underbrace{(-141)}_{c} = 1$

stage 4 $\longrightarrow$ $x = 150 \times 118 \times 331 + 144 \times (-141) \times 277 \pmod{91687}$

$y = \quad$ " $\quad - \quad$ " $\quad$ "

$x \rightarrow 11482908 \pmod n = \overbrace{22033}^{m_2}$ $\quad -x \pmod n = \overbrace{69654}^{m_1}$

$y \rightarrow 234492 \pmod n = \underbrace{51118}_{m_4}$ $\quad -y \pmod n = \underbrace{40569}_{\checkmark m_3}$

$\boxed{\text{Algorithm } X_1:}$ Find square roots (mod) prime p if $\underline{p \equiv 3 \pmod 4}$

Input: odd prime p where $p \equiv 3 \pmod 4$ & "a" $\rightarrow$ (cipher 62111)

$\boxed{4}$ page

output: Two square roots of "a" (mod p)

1. Compute $r = a^{\frac{p+1}{4}} \pmod p$ $\leftarrow$ $\boxed{\text{S-8-M alg}}$

2. return $(r, -r)$

$\boxed{\text{Example}}$

(a prime #) $\rightarrow q = 331 \longrightarrow 331 \equiv 3 \pmod 4$

$r = 62111^{\frac{332}{4}} \pmod{331} = 144 \longrightarrow (\mp 144)$

$\boxed{\text{Algorithm } X_2:}$ Find square roots (mod) prime p if $\underline{p \equiv 5 \pmod 8}$

Input: odd prime p where $p \equiv 5 \pmod 4$ & "a" $\rightarrow$ (cipher 62111)

output: Two square roots of "a" (mod p)

1. compute $d = a^{\frac{p-1}{4}} \pmod p$

2. if $d = 1 \longrightarrow r = a^{\frac{p+3}{8}} \pmod p$

3. if $d = p-1 \longrightarrow r = 2a\,(4a)^{\frac{p-5}{8}} \pmod p$

4. return $(r, -r)$

$\boxed{\text{Example}}$

(a prime #) $\rightarrow p = 277 \longrightarrow 277 \equiv 5 \pmod 8$

$d = 62111^{\frac{276}{4}} \pmod{277} = 276$ which is $(p-1)$

$r = (2 \times 62111) \times (4 \times 62111)^{\frac{272}{8}} \pmod{277} = 150 \longrightarrow (\mp 150)$

General Algorithm

Algo. Finding square roots mod a prime "p"

Input: odd prime p and "a"
output: two square roots of a (mod p)

1. choose random $b \in \mathbb{Z}_p$ Until $b^2 - 4a$ is a quadratic non-residue (mod p)

$$\left(\frac{b^2-4a}{p}\right) = -1$$

2. let f be a polynomial $x^2 - bx + a \in \mathbb{Z}_p$

3. Compute $r = x^{\frac{(p+1)}{2}} \pmod{f}$ → r is an integer in $\mathbb{Z}_p$

4. return $(r, -r)$

not nessasary for this course