Public Key Cryptography III: Rabin & Elgamal

Rabin Cryptosystem

→ security of this system is equivalent to difficulty of factoring
→ essentially RSA with $e = 2$.
→ mainly used for authentication (signatures)

A. Key Generation

Bob randomly chooses 2 large primes p and q, calculates $n = pq$.
public key $= n$. Private key $= (p, q)$.

Note: This is just RSA with $e=2$!

B. Encryption

Given message M, Alice encrypts $C = M^2 \bmod n$.

C. Decryption

Bob decrypts C by finding the square root of $C \bmod n$.
⇒ knowing (p, q) makes this easy; otherwise it is as difficult as factoring n.

4 intermediate factors $x_1 = C^{\frac{p+1}{4}} \bmod p$.

$$x_2 = p - x_1$$
$$x_3 = C^{\frac{q+1}{4}} \bmod q$$
$$x_4 = q - x_3$$

We define $a = qq^{-1} \bmod p$ and $b = pp^{-1} \bmod q$.
Then, 4 possible plaintexts can be calculated:

$M_1 = (ax_1 + bx_3) \bmod n$ $\quad$ $M_3 = (ax_2 + bx_3) \bmod n$
$M_2 = (ax_1 + bx_4) \bmod n$ $\quad$ $M_4 = (ax_2 + bx_4) \bmod n$

Example:

Choose $p = 7$, $q = 11$. $\Rightarrow n = 7 \times 11 = 77$
⇒ public key $= 77$, private key $= (7, 11)$.

Alice encrypts $M = 3$: $C = 3^2 \bmod 77 = 9$.

To decrypt, Bob calculates: $x_1 = 9^2 \bmod 7 = 4 \Rightarrow x_2 = 7 - 4 = 3$.
$x_3 = 9^3 \bmod 11 = (-2)^3 \bmod 11 = -8 \bmod 11 = 3$
$\Rightarrow x_4 = 11 - 3 = 8$

Bob then finds:
$7^{-1} \bmod 11 = 8 \Rightarrow 7(7^{-1} \bmod 11) = 56$
$11^{-1} \bmod 7 = 2 \Rightarrow 11(11^{-1} \bmod 7) = 22$

$11 = 1(7) + 4 \Rightarrow 4 = 11 - 1(7)$
$7 = 1(4) + 3 \Rightarrow 3 = 7 - 1(4)$
$4 = 1(3) + 1 \Rightarrow 1 = 4 - 1(3)$
$= 4 - 1[7 - 1(4)]$
$1 = 2(4) - 1(7)$
$= 2[11 - 1(7)] - 1(7)$
$1 = 2(11) - 3(7)$

$1 \bmod 11 \equiv [2(11) - 3(7)] \bmod 11$
$= -3(7) \bmod 11$
$= (11-3)(7) \bmod 11 = 8(7) = 11$

$1 \bmod 7 \equiv [2(11) - 3(7)] \bmod 7$
$= 2(11) \bmod 7$

Let $a = 22$, $b = 56$.
The four possible plaintexts:

$M_1 = [22(4) + 56(3)] \bmod 77 = 25$ ✗
$M_2 = [22(4) + 56(8)] \bmod 77 = 74$ ✗
$M_3 = [22(3) + 56(3)] \bmod 77 = 3$ ✓
$M_4 = [22(3) + 56(8)] \bmod 77 = 52$ ✗

Advantages of Rabin's Cryptosystem:
+ provable security
+ unless e is small, Rabin's is faster than RSA
  ∵ requires one modular exponentiation
  ↳ decryption requires roughly same duration as RSA

Disadvantages of Rabin's Cryptosystem:
- receiver needs to decide which one of 4 possible plaintexts is the right one.
  ↳ can append messages with known patterns (ex. 20 zeros) to allow easier recognition of plaintext.

Definition:
Let g be a primitive root for $\mathbb{F}_p$ and let h be a nonzero element of $\mathbb{F}_p$. The Discrete Logarithm Problem (DLP) is the problem of finding an exponent x such that

$$g^x \equiv h \pmod{p}.$$

The number x is called the discrete logarithm of h to the base g and is denoted by $\log_g(h)$.

DL Assumption: There is no efficient algorithm (polynomial time) to solve DLP.
* widely believed that this assumption holds.

ElGamal Cryptosystem:

A. Key Generation
→ Alice chooses a prime p and two random numbers g and u, both less than p, where $g \in \mathbb{Z}_p^*$.
→ Alice calculates $y = g^u \bmod p$.

Alice's public key is (p, g, y); her secret key is u.

B. Encryption
→ To encrypt a message M for Alice, Bob chooses random integer k such that $\gcd(k, p-1) = 1$.
→ Bob calculates: $a = g^k \bmod p$.
$b = y^k M \bmod p$.
Cryptogram, $C = (a, b)$. Length of C = 2 × Length of M.

$9^1 \bmod 11 = 9$
$9^2 \bmod 11 = 4$
$9^4 \bmod 11 = 5$
$9^6 \bmod 11 = (5 \times 4) \bmod 11$
$= 20 \bmod 11 = 9$

C. Decryption
→ To decrypt C, Alice calculates $M = ba^{-u} \bmod p$

$11 = 1(9) + 2 \Rightarrow 2 = 11 - 1(9)$
$9 = 4(2) + 1$
$\Rightarrow 1 = 9 - 4(2)$
$= 9 - 4[11 - 1(9)]$
$1 = 5(9) - 4(11)$
$1 \bmod 11 \equiv [5(9) - 4(11)] \bmod 11$
$\equiv 5(9) \bmod 11$
$\Rightarrow 9^{-1} \bmod 11 = 5$

Example:
Suppose Alice chooses prime $p = 11$, generator $g = 3$, and secret key $u = 6$. $y = 3^6 \bmod 11 = 3$.
Public key $= (p, g, y) = (11, 3, 3)$.

To encrypt $M = 6$, Bob chooses $k = 7$ and calculates
$a = 3^7 \bmod 11 = 9$ $\quad b = 3^7(6) \bmod 11 = 10$.
$\Rightarrow$ Cryptogram, $C = (9, 10)$.

To decrypt C, Alice calculates $M = (10/9^6) \bmod 11 = (10/9) \bmod 11 = (10 \times 5) \bmod 11 = 6$.