Public Key Cryptography

Lecture 6

The Rabin Public Key Cryptosystem

Index

1. The Rabin Public Key Cryptosystem
2. Quadratic Residues. Legendre and Jacobi Symbols
3. The Modular Square Root Problem
4. Examples

The Rabin Public Key Cryptosystem

- Rabin (1979)
- based on the Modular Square Root Problem
- the first example of a provably secure public-key cryptosystem

1. Key generation. Alice creates a public key and a private key.

1.1. Generates 2 random large distinct primes p, q of approximately same size.
1.2. Computes $n = p \cdot q$.
1.3. Alice's public key is n; her private key is (p, q).

2. Encryption. Bob sends an encrypted message to Alice.

2.1. Gets Alice's public key n.
2.2. Represents the message as a number m between 0 and $n - 1$.
2.3. Computes $c = m^2 \bmod n$.
2.4. Sends the ciphertext c to Alice.

3. Decryption. Alice decrypts the message from Bob.

3.1. Uses the private key (p, q) to determine the 4 square roots m_1, m_2, m_3, m_4 of c modulo n.
3.2 Decides which one of the 4 messages m_1, m_2, m_3, m_4 is that sent by B.

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$
- the encryption function is $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f(m) = m^2 \bmod n$.
- the decryption function is $f^{-1} : \mathbb{Z}_n \to \mathbb{Z}_n$, $f^{-1}(c) =$ one of the 4 square roots of c modulo n.

Comparison with RSA

- The Rabin encryption takes only a modular squaring, whereas the RSA encryption takes at least a modular squaring and a modular multiplication.
- The Rabin decryption and the RSA decryption are comparable.

Quadratic Residues

Write "$=$" instead of "$\equiv$" and x instead of $\hat{x}$.
In what follows set a prime $p > 2$ and denote $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Definition

An element $a \in \mathbb{Z}_p^*$ is called a quadratic residue modulo p if $\exists b \in \mathbb{Z}_p$ such that $b^2 = a$.

If $b^2 = a$ in $\mathbb{Z}_p^*$, then a has 2 square roots, namely $\pm b$.

Hence the quadratic residues can be found by computing $b^2 \bmod p$ for $b = 1, 2, \ldots, \frac{p-1}{2}$, because the other elements must be congruent modulo p to $-b$ for such an element b.

Therefore, $\mathbb{Z}_p^*$ has exactly $\frac{p-1}{2}$ quadratic residues.

Legendre Symbol

Example. We get the quadratic residues in $\mathbb{Z}_{11}^*$ by computing $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$ and $5^2 = 3$. Notice that $6 = -5$, $7 = -4$, $8 = -3$, $9 = -2$ and $10 = -1$ modulo 11.

Definition

Let $a \in \mathbb{Z}$ and let $p > 2$ be a prime. Then we define the Legendre symbol, denoted by $(\frac{a}{p})$, as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is quadratic residue mod } p \\ -1 & \text{if } a \text{ is non-quadratic residue mod } p \end{cases}$$

The Legendre symbol tell us if an integer is or is not a quadratic residue modulo p.

Legendre Symbol (cont.)

Theorem

Let $a, b \in \mathbb{Z}$ and p, q be odd primes.

(i) $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, *hence* $\left(\frac{b^2}{p}\right) = 1$.

(iii) $\left(\frac{1}{p}\right) = 1$ *and* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

(iv)

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p = \pm 1 \pmod{8} \\ -1 & \text{if } p = \pm 3 \pmod{8} \end{cases}$$

(v) (Law of Quadratic Reciprocity)

$$\begin{aligned} \left(\frac{q}{p}\right) &= (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) \\ &= \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p = q = 3 \pmod{4} \\ \left(\frac{p}{q}\right) & \text{otherwise} \end{cases} \end{aligned}$$

Legendre Symbol (cont.)

In order to check that an integer a is a quadratic residue modulo p, one can evaluate the Legendre symbol for the factors. For that, write $a = 2^k q$, where q is odd and apply (ii), (iv) and (v). Clearly, we may assume that $a < p$, so that $q < p$. Property (v) offers the relationship between $(\frac{q}{p})$ and $(\frac{p}{q})$, the latter one being possible to be reduced.

Example. Let us determine if $n = 7411$ is a quadratic residue modulo $p = 9283$.
Since n is prime and $7411 = 9283 = 3 \pmod 4$, it follows that $\left(\frac{n}{p}\right) = -\left(\frac{p}{n}\right) = -\left(\frac{1872}{7411}\right)$. But since $1872 = 2^4 \cdot 3^2 \cdot 13$, using (iii) we get $(\frac{n}{p}) = -(\frac{13}{7411})$. Since $13 = 1 \pmod 4$, we have $-\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1$. Hence n is not a quadratic residue modulo p.

Disadvantage: factorization.

Jacobi Symbol

One can avoid factorization of odd numbers, using a generalization of the Law of Quadratic Reciprocity, that holds for any odd integer $n \geq 3$.

Definition

Let $a \in \mathbb{Z}$ and let $n \geq 3$ be odd. Let $n = p_1^{k_1} \dots p_r^{k_r}$ be the factorization of n. We define the Jacobi symbol as the product of the Legendre symbols for the prime factors of n, that is,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \dots \left(\frac{a}{p_r}\right)^{k_r}.$$

Note that if $\left(\frac{a}{n}\right) = 1$ for a composite n, in general it does not follow that a is a quadratic residue modulo n. For instance, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, but there is no $x \in \mathbb{Z}$ such that $x^2 = 2 \pmod{15}$.

Jacobi Symbol (cont.)

Theorem

Let $a, b \in \mathbb{Z}$ and $m, n \geq 3$ be odd.
(i) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
(ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, *hence* $\left(\frac{b^2}{n}\right) = 1$.
(iii) $\left(\frac{1}{n}\right) = 1$ *and* $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
(iv)

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} 1 & \text{if } n = \pm 1 \pmod 8 \\ -1 & \text{if } n = \pm 3 \pmod 8 \end{cases}$$

(v) (Law of Quadratic Reciprocity)

$$\begin{aligned} \left(\frac{m}{n}\right) &= (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right) \\ &= \begin{cases} -\left(\frac{n}{m}\right) & \text{if } n = m = 3 \pmod 4 \\ \left(\frac{n}{m}\right) & \text{otherwise} \end{cases} \end{aligned}$$

Jacobi Symbol (cont.)

Example. Let us determine if $n = 7411$ is a quadratic residue modulo $p = 9283$.
Since n is prime and $7411 = 9283 = 3 \pmod 4$, it follows that $\left(\frac{n}{p}\right) = -\left(\frac{p}{n}\right) = -\left(\frac{1872}{7411}\right)$ as in the previous example. Now we do not factorize 1872, but factor out only the power of 2.

$$\left(\frac{n}{p}\right) = -\left(\frac{1872}{7411}\right) = -\left(\frac{2^4}{7411}\right)\left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right) = -\left(\frac{40}{117}\right)$$

$$= -\left(\frac{2^3}{117}\right)\left(\frac{5}{117}\right) = -\left(\frac{2}{117}\right)\left(\frac{5}{117}\right) = \left(\frac{5}{117}\right) = \left(\frac{117}{5}\right) = \left(\frac{2}{5}\right) = -1\,.$$

Theorem

The complexity of the algorithm of computing the Jacobi symbol is $O(\log^2 n)$.

The Modular Square Root Problem

Problem

Given $a \in \mathbb{Z}$ and an odd $n = p \cdot q \in \mathbb{N}$ $(n \geq 3)$ for some primes p and q, determine x such that

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

Splitting the problem in 2 steps

- I. Square root modulo p (p prime).
- II. Square root modulo n ($n \in \mathbb{N}$, $n \geq 3$ odd).

Theorem

Modular Square Root Problem is essentially computationally equivalent to Integer Factorization Problem.

Remark. (i) Using the Law of Quadratic Reciprocity, we can quickly determine if $a \in \mathbb{Z}$ is a quadratic residue modulo p. Then we only know that

$$x^2 = a \pmod{p} \tag{1}$$

has a solution and not which one is that solution.
(ii) (1) has exactly 2 solutions; if x is a solution, then so is $-x$.
(iii) Since we are interested in large primes, we discuss only the case when the prime p is odd.

Cases

- $p = 1 \pmod{8}$
- $p = 3 \pmod{4}$ (that is, $p = 3 \pmod{8}$ or $p = 7 \pmod{8}$)
- $p = 5 \pmod{8}$

I. Square Root Modulo p (cont.)

- **The case $p = 1 \pmod 8$.**

  1. Write $p - 1 = 2^s t$ where t is odd.
  2. Randomly find a quadratic non-residue modulo p, say d, such that $2 \leq d \leq p - 1$.
  3. Compute $A := a^t \bmod p$.
  4. Compute $D := d^t \bmod p$.
  5. Determine $D^{-1} \bmod p$.
  6. Compute even powers $2k$ of D^{-1}, for $0 \leq k < 2^{s-1}$, until we get $D^{-2k} = A \pmod p$.
  7. A solution is $x = a^{\frac{t+1}{2}} D^k \pmod p$.

- **The case $p = 3 \pmod 4$.**

  A solution is $x = a^{\frac{p+1}{4}} \pmod p$.

- **The case $p = 5 \pmod 8$.**

  A solution is

$$\begin{cases} x = a^{\frac{p+3}{8}} \pmod p & \text{if } a^{\frac{p-1}{4}} = 1 \pmod p \\ x = 2a \cdot (4a)^{\frac{p-5}{8}} \pmod p & \text{otherwise} \end{cases}$$

I. Square Root Modulo p (cont.)

Example. Let us determine a square root modulo $p = 2081$ of $a = 302$.

Step 0. Check that a is a quadratic residue modulo p.

We have

$$\begin{aligned}
\left(\frac{302}{2081}\right) &= \left(\frac{2}{2081}\right)\left(\frac{151}{2081}\right) = \left(\frac{151}{2081}\right) = \left(\frac{2081}{151}\right) = \left(\frac{118}{151}\right) \\
&= \left(\frac{2}{151}\right)\left(\frac{59}{151}\right) = \left(\frac{59}{151}\right) = -\left(\frac{151}{59}\right) = -\left(\frac{33}{59}\right) \\
&= -\left(\frac{3}{59}\right)\left(\frac{11}{59}\right) = (-1)(-1)\left(\frac{59}{3}\right)(-1)\left(\frac{59}{11}\right) \\
&= -\left(\frac{2}{3}\right)\left(\frac{4}{11}\right) = (-1)\cdot(-1)\cdot 1 = 1
\end{aligned}$$

Note that $p = 1 \pmod 8$.

Step 1. Write $p - 1 = 2^s t$ where t is odd.

We have $2080 = 2^5 \cdot 65$, so $s = 5$ and $t = 65$.

Step 2. Look for a quadratic non-residue d modulo p.
In practice, d is randomly chosen. Here we try $d = 2, 3, \ldots$.
We have

$$\left(\frac{2}{2081}\right) = 1, \quad \left(\frac{3}{2081}\right) = \left(\frac{2081}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

hence $d = 3$ is a quadratic non-residue modulo p.
Step 3. Compute $A = a^t \bmod p$.
$A = 302^{65} \bmod 2081 = \cdots = 102$
(by repeated squaring modular exponentiation).
Step 4. Compute $D = d^t \bmod p$.
$D = 3^{65} \bmod 2081 = \cdots = 888 \pmod{2081}$
(by repeated squaring modular exponentiation).
Step 5. Determine $D^{-1} \bmod p$.
$888^{-1} \bmod 2081 = \cdots = 1310 \pmod{2081}$
(by the extended Euclidean algorithm).

Step 6. Compute even powers $2k$ of D^{-1}, for
$0 \leq k < 2^{s-1} = 2^4 = 16$, until $D^{-2k} = A \pmod{p}$.
We have

$$\begin{aligned} D^{-2} &= 1310 \cdot 1310 = 1356 \pmod{2081} \\ D^{-4} &= 1356 \cdot 1356 = 1213 \pmod{2081} \\ D^{-6} &= 1356 \cdot 1213 = 838 \pmod{2081} \\ D^{-8} &= 1213 \cdot 1213 = 102 \pmod{2081} \end{aligned}$$

Thus $D^{-8} = A$, hence $k = 4$.
Step 7. A solution is

$$x = a^{\frac{t+1}{2}} D^k = 302^{33} \cdot 888^4 = \cdots = 1292.$$

(by repeated squaring modular exponentiation)
Therefore, a square root modulo $p = 2081$ of $a = 302$ is $x = 1292$.
The other solution between 0 and $p - 1 = 2080$ is $-x = 789$.
It is easy to check that $x^2 = a \pmod{p}$.

I. Square Root Modulo p (cont.)

- There is no *deterministic* polynomial-time algorithm to find a quadratic non-residue modulo p.
- A randomly chosen d has a 50% chance of being a quadratic non-residue and this can be checked in polynomial time.
- The previous algorithm (due to Tonelli and Shanks) is *probabilistic*, although its only non-deterministic part is finding a quadratic non-residue modulo p.
- One could make it completely deterministic by successively trying $d = 2, 3, \ldots$ in Step 2 until a quadratic non-residue is find. Unfortunately, it can be proved that the smallest quadratic non-residue is of order $O(p^\alpha)$ for some $\alpha \neq 0$, hence we get an exponential-time algorithm.

Theorem

Given a quadratic non-residue modulo a prime p, the complexity of the algorithm of extracting the square root modulo p is $O(\log^4 p)$.

II. Square Root Modulo n

Now let us see how to solve the general problem

$$x^2 = a \pmod{n} \tag{3}$$

for any odd $n = p \cdot q \in \mathbb{N}$ ($n \geq 3$.

Given the factorization $n = p \cdot q$, (3) can be solved as follows:

- Solve $x^2 = a \pmod{p}$ and $x^2 = a \pmod{q}$.
- Use the Chinese Remainder Theorem to get a solution modulo n.

Remark. Problem (3) has solution only if a is a quadratic residue modulo p and modulo q.

II. Square Root Modulo n (cont.)

Theorem

Modular Square Root Problem is essentially computationally equivalent to Integer Factorization Problem.

Proof. Given the factorization, one can compute modular square roots by the method above.
Conversely, suppose that we have an algorithm to compute modular square roots.

- We choose a random number x and apply the algorithm to the least positive residue of $x^2 \bmod n$. Hence we have $x'^2 \equiv x^2 \pmod{n}$ for some number x'.
- We have a 50% chance that $x' \not\equiv \pm x \pmod{n}$, in which case a non-trivial factor is obtained: $(x' + x, n)$ or $(x' - x, n)$.
- By repeating this procedure k times, we have a probability $1 - \frac{1}{2^k}$ of factoring n.

Rabin - examples

Example. General setting:

- Use the Rabin cryptosystem.
- Use a 27-letters alphabet for plaintext and ciphertext: _ (blank) with numerical equivalent 0 and letters $A-Z$ (the English alphabet) with numerical equivalents 1-26.

_	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Plaintext message units are blocks of k letters, whereas ciphertext message units are blocks of l letters. The plaintext is completed with blanks, when necessary.
- We must have $27^k < n < 27^l$.

Rabin - examples (cont.)

Let $k = 2$, $l = 3$ and $K_D = (p, q) = (31, 53)$.

- Ciphertext: BED_HI
- Split the ciphertext: BED /_HI
- Consider the first trigraph.
- Write the numerical equivalent:
  BED $\mapsto 2 \cdot 27^2 + 5 \cdot 27 + 4 = 1597$
- Solve $x^2 = 1597 \pmod{31}$ and $x^2 = 1597 \pmod{53}$, that is,
  (i) $x^2 = 16 \pmod{31}$,
  (ii) $x^2 = 7 \pmod{53}$.
  Clearly, (i) has solutions ± 4 modulo $p = 31$.
  Let us solve (ii). We have $q = 53 = 5 \pmod 8$ and
  $a^{\frac{q-1}{4}} = 7^{\frac{53-1}{4}} = -1 \pmod{53}$, hence (ii) has solutions modulo $q = 53$

$$\pm 2a \cdot (4a)^{\frac{p-5}{8}} = \pm 2 \cdot 7 \cdot (4 \cdot 7)^{\frac{53-5}{8}} = \cdots = \pm 22\,.$$

Rabin - examples (cont.)

- Solve $x^2 = 1597 \pmod{n}$, where $n = p \cdot q$.
  We have to solve the systems

$$\begin{cases} x = \pm 4 \pmod{31} \\ x = \pm 22 \pmod{53} \end{cases}$$

Chinese Remainder Theorem

Consider the system

$$\begin{cases} x = a_1 \pmod{n_1} \\ \dots\dots\dots \\ x = a_r \pmod{n_r} \end{cases}$$

where each $a_i, n_i \in \mathbb{N}$, $n_i \neq 0$ and $(n_i, n_j) = 1$, $\forall i, j \in \{1, \dots, r\}$, $i \neq j$.
Then the system has unique solution modulo $N = n_1 n_2 \dots n_r$, namely
$x = \sum_{i=1}^{r} a_i N_i K_i$, where $N_i = N/n_i$ and $K_i = N_i^{-1} \bmod n_i$, $i = 1, \dots, r$.

Rabin - examples (cont.)

Here $N = n = 31 \cdot 53 = 1643$, $N_1 = 53$, $N_2 = 31$,
$K_1 = N_1^{-1} \bmod 31 = \ldots = 24$, $K_2 = N_2^{-1} \bmod 53 = \ldots = 12$.
The 4 solutions modulo $N = 1643$ of the systems are given by

$$\begin{aligned} a_1 N_1 K_1 + a_2 N_2 K_2 &= \pm 4 \cdot 53 \cdot 24 + (\pm 22) \cdot 31 \cdot 12 \\ &= \pm 5088 \pm 8184, \end{aligned}$$

hence $x_1 = 128$, $x_2 = 1453$, $x_3 = 1515$, $x_4 = 190$.
Since $x_2, x_3 \geq 27^2$, they are not good.

- Write the literal equivalents:
  $x_1 = 128 = 4 \cdot 27 + 20 \mapsto$ DT
  $x_4 = 190 = 7 \cdot 27 + 1 \mapsto$ GA
  The second one is an acceptable solution.
- Similarly, one decrypts the second trigraph, getting ME.
- Plaintext: GAME

Rabin - examples (cont.)

Example. Let $K_D = (p, q) = (277, 331)$, hence $n = p \cdot q = 91687$. Suppose that we replicate the last 6 bits of the original message block.

- *Encryption.* Let $m_0 = 633$, that is, $m_0 = (1001111001)_2$. Replicate the last 6 bits to get $m = (10011110011111001)_2$, that is, $m = 40569$.
  Compute $c = m^2 \bmod n = 40569^2 \bmod 91687 = 62111$.
- *Decryption.* To decrypt, use the above method and get the roots $m_1 = 69654$, $m_2 = 22033$, $m_3 = 40569$, $m_4 = 51118$ of c modulo n, that is,
  $m_1 = (10001000000010110)_2$,
  $m_2 = (10101100000010001)_2$,
  $m_3 = (10011110011111001)_2$,
  $m_4 = (11000111110101110)_2$.
  Since only m_3 has the required redundancy, get the original message $m_0 = (1001111001)_2$, that is, $m_0 = 633$.

Selective Bibliography

- H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.
- N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. [http://www.cacr.math.uwaterloo.ca/hac]