The Rabin Cryptosystem

Naiara Escudero Sanchez
naiara.escudero@googlemail.com
University of Paderborn

Abstract

Since the communications between people exists, the necessity of that the exchanged messages can be interpreted only for a certain group of people also exists. This necessity and the fact that exchanged messages are exposed to other people during the transmission promoted the creation of encryption systems, enabling just the recipients to interpret the exchanged information.

In this paper, a particular cryptosystem called Rabin Cryptosystem is presented and analyzed. Also, before that, some basic mathematical concepts and theorems are explained to make possible understand the cryptosystem. Finally it is compared with RSA cryptosystem in terms of security and efficiency.

1. Introduction

Since the appearance of the first encryption systems, the evolution of this science called cryptography doesn't stop to grow day by day. The first cryptography methods are very far from the complex cryptosystems used now.

In general, the cryptosystems can be divided into two basic types: Symmetric Key Encryption and Asymmetric Key Encryption. The first one uses the same key to encrypt and decrypt, so the key must be kept private and the major challenge is the secure distribution of it. The second one uses two keys, a private key and a public key. The information is encrypted with one of them and decrypted with the other one. The Rabin cryptosystem belongs to the asymmetric key encryption group.

In the following Figures, we can see the basic scheme of the encrypt and decrypt processes in a symmetric and asymmetric key encryption correspondingly:

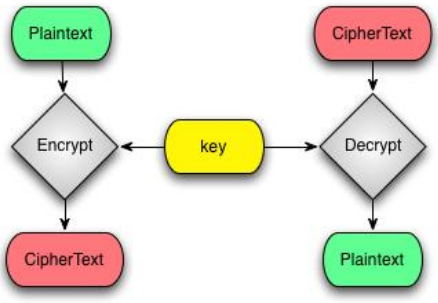


Figure 1. Symmetric system[3]

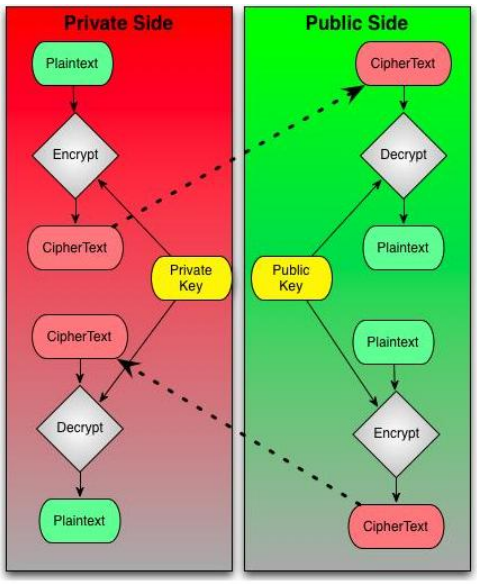


Figure 2. Asymmetric system[3]

The goal of this paper is to introduce and explain the Rabin cryptosystem, how it works, which idea it is based on and its security.

The rest of the paper is organized as follows. In section II the motivation of this paper is explained. The main section, the Section III is used to explain some basic mathematical concepts necessary to understand

the Rabin cryptosystem, followed by the presentation of the cryptosystem and a evaluation of its security. Section IV compares the Rabin cryptosystem with the RSA cryptosystem in terms of security and efficiency. And finally, the paper is concluded in the Section V.

2. Motivation

The privacy of the messages in the communications is not a solved problem. Just as there are algorithms for occulting the information by encrypting it, there exist other algorithms able to decrypt the information and enable unauthorized persons to access the information. For that reason, the cryptography is a crucial branch of the communications that requires continuous research causing its evolving. It is vital to be able to ensure the privacy of the information exchanged in the communications.

This work is motivated by the seminar Complexity and cryptography, which focuses on the most important cryptosystems and some aspects of the complexity theory.

3. The Rabin Cryptosystem

The Rabin Cryptosystem is an asymmetric key encryption based on number-theoretic problems related to the hardness of factoring. For that reason, some number theory has to be present before we can explain the cryptosystem.

In this section the basic mathematical concepts needed to understand the cryptosystem are introduced. Some examples will be shown for a better comprehension, and finally, the evaluation of the degree of security provided by our cryptosystem will be shown.

3.1. The Chinese Remainder Theorem

The Chinese remainder theorem is a method of solving systems of congruences:

Theorem 1 (Chinese Remainder Theorem)**.** Let r and s be positive integers which are relatively prime and let a and b be any two integers. Then there is an integer N such that:

$$N \equiv a \mod r \text{ and } N \equiv b \mod s$$

Moreover, N is uniquely determined modulo $r \cdot s$. The theorem can be generalized as follows. Given a set of simultaneous congruences:

$$x \equiv a_i \mod m_i$$

for $i = 1, ..., r$ and for which the m_i are pairwise relatively prime, the solution of the set of congruences is:

$$x \equiv a_1 b_1 \tfrac{M}{m_1} + ... + a_r b_r \tfrac{M}{m_r} \mod M$$

where $M = m_1 m_2 ... m_r$ and $\frac{M}{m_i} \cdot b_i \equiv 1 \mod m_i$.

3.2. Quadratic Residues

The discussion of quadratic residues will be divided into two parts: quadratic residues modulo a prime p, and the quadratic residues modulo a composite N, where p and q are odd primes and N = pq.

3.2.1. Quadratic Residues Modulo a Prime. Let G be a group. An element $y \in G$ is called quadratic residue if there exists another element $x \in G$ such that:

$$x^2 = y$$

If there is no such x, then y is called a quadratic non-residue. In this case QR_q denotes the set of quadratic residues of a given group and QNR_q the quadratic non-residues . Also, when the given group is Z_q^* for a prime q, the element y is a quadratic residue if:

$$x^2 = y \mod q$$

Example: Lets go to compute the quadratic residues $\mod 11$. Computing the range of numbers $0 \leq x \leq \frac{q}{2}$ is enough for reason of symmetry:

n	1	2	3	4	5	6	7	8	9	10
$n^2 \mod 11$	1	4	9	5	3	3	5	9	4	1

$1 \to 1^2 = 1 \to 1 \mod 11 = 1$
$2 \to 2^2 = 4 \to 4 \mod 11 = 4$
$3 \to 3^2 = 9 \to 9 \mod 11 = 9$
$4 \to 4^2 = 16 \to 16 \mod 11 = 5$
$5 \to 5^2 = 25 \to 25 \mod 11 = 3$

So, we can conclude that the elements belonging to Z_q^* which are quadratic residues $\mod 11$ are the set of elements {1, 3, 4, 5, 9} and the non-quadratic residues $\mod 11$ the elements {2, 6, 7, 8, 10}.

Theorem 2. Let q $>$ 2 be a prime. Then every quadratic residue has exactly two square roots and the number of solutions are:

- 1 solution if $y = 0$.
- 2 solutions if $y \neq 0$.

Proof: Let $y \in Z_q^*$ be a QR_q. By definition, there exists an $x \in Z_q^*$ such: $x^2 = y \mod q$ and $(-x)^2 = x^2 = y \mod q$. Furthermore, $-x \neq x \mod q$: if $-x = x \mod q$, then $2x = 0 \mod q$ which implies $q|2x$. This means that either $q|2$ or $q|x$, both impossible since q is prime > 2 and $0 < x < q$. Therefore $[x \mod q]$ and $[-x \mod q]$ must be different elements of Z_q^*, so y has at least two square roots.

Now, let $x, z \in Z_q^*$ be square roots of y. Then $x^2 = y = z^2 \mod q$, which means that $x^2 - z^2 = 0 \mod q$. Hence $(x-z)(x+z) = 0 \mod q$. Since q is a prime either $q|(x-z)$ or $q|(x+z)$. In the first case, $z = x \mod q$ and in the second case $z = -x \mod q$, showing that y has only the square roots: $[\pm x \mod q]$. □

Theorem 3. The number of quadratic residues and quadratic non-residues in Z_q^* is equal:

$$|QR_q| = |QNR_q| = \frac{|Z_q^*|}{2} = \frac{(q-1)}{2}$$

Proof: Let Z_q^* a cyclic group of order $q-1$ and let g be a generator of this group, that means that:

$$Z_q^* = \{g^1, g^2, ..., g^{q-1}\}$$

As q is odd, $q-1$ must be even. So half of all elements between 1 and $q-1$ have an even exponent. Since $2|j$, being j an even number, for half of the all elements in $\{g^1, g^2, ..., g^{q-1}\}$ we have that $g^{\frac{i}{2}} \in Z_q^*$ for some even integer i. So finally, we can conclude that half of all elements are QR. □

Example: If we continue with the previous example, but we compute all numbers, we get:

n	1	2	3	4	5	6	7	8	9	10
$n^2 \mod 11$	1	4	9	5	3	3	5	9	4	1

As we can see, each quadratic equation $\mod 11$ has exactly two solutions. For example, the equation $x^2 = 4 \mod 11$ has the solutions 2 and 9, or the equation $x^2 = 9 \mod 11$ has the solutions 3 and 8.

Also, we can see that there are the same number of quadratic residues and quadratic non-residues:

$\{1, 3, 4, 5, 9\} \in QR_{11}$
$\{2, 6, 7, 8, 10\} \in QNR_{11}$
$\frac{(q-1)}{2} = \frac{(11-1)}{2} = 5$

One way to express if an element y is a quadratic or non-quadratic residue mod q is using the Legendre symbol:

$$L_q(y) = \begin{cases} +1 & \text{if } y \in QR_q \\ -1 & \text{if } y \in QNR_q \end{cases}$$

Theorem 4. Let q > 2 be a prime. Then:

$$L_q(y) = y^{\frac{q-1}{2}} \mod q$$

Proof: As we proofed before, a quadratic residue x modulo q can be expressed as: $x = g^i$ for some even integer i and an arbitrary generator g of Z_q^*. If we suppose now $i = 2j$ with j an integer:

$$x^{\frac{(q-1)}{2}} = (g^{2j})^{\frac{(q-1)}{2}} = g^{(q-1)j} = (g^{q-1})^j = 1^j = 1 \mod q$$

We have shown that $x^{\frac{(q-1)}{2}} = 1 = L_q(x) \mod q$. Now, if $x \in QNR_q : x = g^i$ for some odd integer i. Let now $i = 2j+1$. Then:

$$x^{\frac{(q-1)}{2}} = (g^{2j+1})^{\frac{(q-1)}{2}} = (g^{2j})^{\frac{(q-1)}{2}} g^{\frac{(q-1)}{2}} = g^{\frac{(q-1)}{2}} = g^{\frac{(q-1)}{2}} \mod q$$

Now:

$$(g^{\frac{(q-1)}{2}})^2 = g^{q-1} = 1 \mod q$$

and so $g^{\frac{(q-1)}{2}} = \pm \mod q$ since $[\pm 1 \mod q]$ are the two square roots of 1. Since g is a generator, $g^{\frac{(q-1)}{2}} \neq 1 \mod q$, and that means that:

$$x^{\frac{q-1}{2}} = -1 = L_p(x) \mod p$$

□

Example: Let's go to apply the Legendre theorem to some elements:

$L_{11}(4) = 4^5 \mod 11 = 1 \Rightarrow 4 \in QR_{11}$
$L_7(2) = 2^3 \mod 7 = 1 \Rightarrow 2 \in QR_7$

From these propositions, it is possible to derive an algorithm for checking if a determined element y is a quadratic residue or not:

$$y^{\frac{q-1}{2}} \mod q = \begin{cases} +1 & \text{if } y \in QR_q \\ -1 & \text{if } y \in QNR_q \end{cases}$$

Example:

$1^5 \mod 11 \Leftrightarrow 1 \mod 11 = 1 \Rightarrow 1 \in QR_q$
$2^5 \mod 11 \Leftrightarrow 32 \mod 11 = 10 \Rightarrow 2 \in QNR_q$
$3^5 \mod 11 \Leftrightarrow 243 \mod 11 = 1 \Rightarrow 3 \in QR_q$
$4^5 \mod 11 \Leftrightarrow 1024 \mod 11 = 1 \Rightarrow 4 \in QR_q$
$6^5 \mod 11 \Leftrightarrow 7776 \mod 11 = 10 \Rightarrow 5 \in QNR_q$

Finally, the quadratic residues follow a property called multiplicative property of quadratic residues.

Theorem 5. Let $q > 2$ be a prime and $x, y \in Z_q^*$. Then:

$$L_q(xy) = L_q(x)L_q(y)$$

Proof:
$L_q(xy) = (xy)^{\frac{q-1}{2}} = x^{\frac{q-1}{2}} y^{\frac{q-1}{2}} = L_q(x)L_q(y) \mod q$

Since $L_q(xy), L_q(x), L_q(y) = \pm 1$ equality holds over the integers as well. □

Using the previous theorem it is possible to derive:

$$xx' \in QR_q$$
$$y'y \in QR_q$$
$$xy \in QNR_q$$

where $x, x' \in QR_q$ and $y, y' \in QNR_q$.

3.2.2. Quadratic Residues Modulo a Composite. Now, the elements belong to the group Z_N^*, where $N = pq$ with p,q distinct primes. Applying the Chinese remainder theorem, Z_N^* can be expressed as:

$$Z_N^* = Z_p^* \times Z_q^*$$

then, an element belonging to this group is denoted by:

$$y \leftrightarrow (y_p, y_q)$$

where $y_p = y \mod p$ and $y_q = y \mod q$.

Theorem 6. An element y is a quadratic residue modulo N if and only if y_p is a quadratic residue $\mod p$, and y_q is a quadratic residue $\mod q$.

Proof: Let $y \in QR_N$ and $x \in Z_N^*$ such that $x^2 = y \mod N$. Then:

$$(y_p, y_q) \leftrightarrow y = x^2 \leftrightarrow (x_p, x_q)^2$$
$$= ([x_p^2 \mod p], [x_q^2 \mod q])$$

We have shown that:

$$y_p = x_p^2 \mod p \text{ and } y_q = x_q^2 \mod q$$

and y_p and y_q are quadratic residues modulo p and q respectively. On the otherhand, if $y \leftrightarrow (y_p, y_q)$ and y_p, y_q are quadratic residues respectively, then there exist $x_p \in Z_p^*$ and $x_q \in Z_q^*$ such that $x \leftrightarrow (x_p, x_q)$, $x \in Z_N^*$. Then, reversing the steps we have shown that x is a square root of $y \mod N$. □

Example: Let $q = 3$ and $p = 5$, then $N = 15$. First we have to compute the quadratic residues modulo 3 and modulo 5:

Z_3^* :
$1 : 1^1 \mod 3 = 1$
$2 : 2^1 \mod 3 = 2 \rightarrow \{1\} \in QR_3$

$Z5*$:
$1 : 1^2 \mod 5 = 1$
$2 : 2^2 \mod 5 = 4$
$3 : 3^2 \mod 5 = 4$
$4 : 4^2 \mod 5 = 1 \rightarrow \{1, 4\} \in QR_5$

Now, we can compute the quadratic residues modulo $N = 15$.

$1 : 1^1 \mod 3 = 1; 1^2 \mod 5 = 1 \rightarrow 1 \in QR_{15}$
$2 : 2^1 \mod 3 = 2; 2^2 \mod 5 = 4$
$4 : 4^1 \mod 3 = 1; 4^2 \mod 5 = 1 \rightarrow 4 \in QR_{15}$
$7 : 7^1 \mod 3 = 1; 7^2 \mod 5 = 4$
$8 : 8^1 \mod 3 = 2; 8^2 \mod 5 = 4$
$11 : 11^1 \mod 3 = 2; 11^2 \mod 5 = 1$
$13 : 13^1 \mod 3 = 1; 13^2 \mod 5 = 4$
$14 : 14^1 \mod 3 = 2; 14^2 \mod 5 = 1$

Then:$\{1, 4\} \in QR_{15}^*$

Now, each quadratic residue $y \in QR_N$ has four square roots unlike the two square roots that the quadratic residues $x \in QR_q$ had. These square roots are given by the elements:

$$(x_p, x_q), (-x_p, x_q), (x_p, -x_q), (-x_p, -x_q)$$

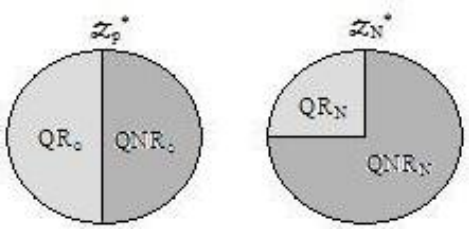
Example: the element 4 is a quadratic residue $\mod 15 : 2^2 = 4 \mod 15$. The square roots are given by:

n	1	**2**	4	**7**	**8**	11	**13**	14
$n^2 \mod 15$	1	**4**	1	**4**	**4**	1	**4**	1

$(2 \mod 5, 2 \mod 3) = (2, 2) \leftrightarrow 2$
$(2 \mod 5, -2 \mod 3) = (2, 1) \leftrightarrow 7$
$(-2 \mod 5, 2 \mod 3) = (3, 2) \leftrightarrow 8$
$(-2 \mod 5, -2 \mod 3) = (3, 1) \leftrightarrow 13$

As a consequence of this proposition, it is possible to conclude that only the fourth part of the elements of Z_N^* are quadratic residues, since squaring modulo N is a four-to-one function or since $y \in Z_N^*$ is a quadratic residue if and only if y_p and y_q are quadratic residues modulo Z_p^* and Z_q^* respectively. So there is a correspondence between QR_N and QR_q x QR_p:

$$\frac{|QR_N|}{|Z_N^*|} = \frac{|QR_p||QR_q|}{|Z_N^*|} = \frac{\frac{(p-1)}{2}\frac{(q-1)}{2}}{(p-1)(q-1)} = \frac{1}{4}$$



Example: As we compute before:
$\{1, 2, 4, 7, 8, 11, 13, 14\} \in Z_{15}^* \rightarrow 8$ elem.
$\{1, 4\} \in QR_{15}^* \rightarrow 2$ elem

$\{2, 7, 8, 11, 13, 14\} \in QNR_{15}^* \rightarrow 6$ elem.

It is possible to extend the definition of Legendre symbol to the case of a composite N, being now called the Jacoby symbol:

$$J_N(x) = J_p(x)J_q(x) = x^{\frac{p-1}{2}} \mod p \;\; x^{\frac{q-1}{2}} \mod q$$

In the case modulo a prime p, $Lp(x) = 1$, meant that $x \in QR_p$, otherwise, $Lp(x) = -1$ meant that $x \in QNR_p$. In contrast, in this case that is not true. As we know, $x \leftrightarrow (x_p, x_q) \in QR_N$ only if $x_p \in QR_p$ and $x_q \in QR_q$, that is:

$$J_p(x_p) = J_q(x_q) = 1 = J_N(x)$$

If x is a quadratic residue moduo N, then $J_N(x) = 1$. But also this result can occur if $x_p \in QNR_p^*$ and $x_q \in QNR_q^*$:

$$J_p(x) = J_q(x) = -1 \rightarrow J_N(x) = J_p(x)J_q(x) = 1$$

Then, we can conclude that the Jacoby symbol of $x \mod N$ must be 1 if $x \in QR_N^*$, but on the other side, the value 1 not ensure that $x \in QR_N^*$.

Despite this conclusion, there is also an algorithm able to recognize quadratic residuosity modulo a composite of known factorization, N:

$$y^{\frac{q-1}{2}} \mod q = y^{\frac{p-1}{2}} modp = \begin{cases} 1 & \text{if } y \in QR_N \\ else & \text{if } y \in QNR_q \end{cases}$$

Example: Assume N = pq = 3 x 5. Let's go to apply the algorithm to find it out if the next elements are quadratic residues modulo 15 or not:
$(1^1 \mod 3)(1^2 \mod 5) \rightarrow 1$ x1 $= 1 \rightarrow 1 \in QR_{15}$
$(2^1 \mod 3)(2^2 \mod 5) \rightarrow 2$ x $4 \neq 1 \rightarrow 2 \in QNR_{15}$
$(3^1 \mod 3)(3^2 \mod 5) \rightarrow 0$ x $4 \neq 1 \rightarrow 3 \in QNR_{15}$
$(4^1 \mod 3)(4^2 \mod 5) \rightarrow 1$ x $1 = 1 \rightarrow 4 \in QR_{15}$

The quadratic residues modulo a N, also follow the multiplicative property. In this case:

Theorem 7. Let N = pq be a product of distinct, odd primes and $x, y \in Z_N^*$. Then

$$J_N(xy) = J_N(x)J_N(y)$$

Proof:
$J_N(xy) = J_p(xy)J_q(xy) = J_p(x)J_p(y)J_q(x)J_q(y) = J_p(x)J_q(x)J_p(y)J_q(y) = J_N(x)J_N(y)$ □

Theorem 8. N = pq be a product of distinct, odd primes and $x, x' \in QR_N$ and $y, y' \in QNR_N$. Then:
$xx' \mod N \in QR_N$
$y'y \mod N \in QR_N$
$xy \mod N \in QNR_N$

Proof: Since $x' \in QR_N$ and $x \in QR_N$, we have that:

$$J_p(x) = J_p(x') = 1 \text{ and } J_q(x) = J_q(x') = 1$$

And then:

$$J_p(xx') = J_p(x)J_q(x') = 1$$
$$J_q(xx') = J_q(x)J_q(x') = 1$$

so $J_N(xx') = J_p(xx')J_q(xx') = 1$. As xx' is a quadratic residue modulo p and modulo q, then, xx' must be a quadratic residue modulo N also.

Following the same procedure we have now $x \in QR_N$ and $y \in QNR_N$, so:

$$J_p(x) = J_q(x) = 1 \text{ and } J_p(y) = \pm 1 \text{ and } J_q(y) = \pm 1$$

Then:

$$J_p(xy) = J_p(x)J_q(y) = +1 \text{ or } -1$$
$$J_q(xy) = J_q(x)J_q(y) = -1 \text{ or } +1$$

and $J_N(xy) = J_p(xy)J_q(xy) = \pm 1$, but now xy cannot be a quadratic residue modulo N since $J_p(xy) = -1$ or $J_q(xy) = -1$. That means that $xy \in QNR_N$. □

3.3. The Rabin Cryptosystem

The previous section shows how it is possible to recognize a quadratic residue modulo N if the factorization N is known. The Rabin Cryptosystem is based on the idea that computing square roots modulo a composite N is simple when the factorization is known, but very complex when it is unknown.

The Rabin cryptosystem is an asymmetric system, so requires two different keys, a public key and a private key, one to encrypt the text and the other one to decrypt it.

The first step is to choose the key which is defined by:

$$K = \{n, p, q\}$$

where p and q are primes such that $p, q \equiv 3 \mod 4$, which are the private key. The public key is $n = pq$. Then, to encrypt the message m, the encryption function is applied:

$$e_K(m) = m^2 \mod n = c$$

the result is the ciphertext, c. Now the encoded message can be sent. Once the message reaches the destination, it must be decrypted. For that, the decryption function is applied:

$$d_K(c) = \sqrt{c} \mod n.$$

Since the encryption function e_K is not an injection function, the decryption is not ambiguous. There exist four square roots of $c \mod n$ ($c = m^2 \mod n$), so there are four possible messages, m.

The decryption try to determine m such that:

$$m^2 \equiv c \mod n$$

and this is equivalent to solving the two congruences:

$$z^2 = c \mod p$$
$$z^2 = c \mod q$$

Then:

$$m_p = c^{\frac{p+1}{4}} \mod p$$
$$m_q = c^{\frac{q+1}{4}} \mod q$$

Finally, the four square roots of $c \mod n$ can be computed applying the **Chinese remainder theorem** to the system of congruences:

$$+m_p \mod p$$
$$-m_p \mod p$$
$$+m_q \mod q$$
$$-m_q \mod q$$

Example: Let $n = 77 = pq = 11 \cdot 7$ and $m = 32$. First, the message m must be encoded using the encryption function:

$$e_K(32) = 32^2 \mod 77 = 23 = c$$

The encoded message c = 23 is sent. The receiver must decrypt the message, so has to find the square roots of 23 modulo 7 and modulo 11. The decryption algorithm is applied:

$$m_p = c^{\frac{p+1}{4}} \mod p = 23^{\frac{7+1}{4}} \mod 7 = 4$$
$$m_q = c^{\frac{q+1}{4}} \mod q = 23^{\frac{11+1}{4}} \mod 11 = 1$$

and the system of congruences $x \equiv a_i b_i \frac{M}{m_i}$ is:

$$+m_p \mod p = 4 \mod 7$$
$$-m_p \mod p = 3 \mod 7$$
$$+m_q \mod q = 1 \mod 11$$
$$-m_q \mod q = 10 \mod 11$$

Finally we can apply the Chinese remainder theorem to compute the four square roots:

First we compute b_1 and b_2 such:

$\frac{N}{7} \cdot b_1 \equiv 1 \mod 7 \rightarrow b_1 = 2$
$\frac{N}{11} \cdot b_2 \equiv 1 \mod 11 \rightarrow b_2 = 8$

Now, we can compute the solutions

1) $x \equiv 4 \mod 7$ and $x \equiv 1 \mod 11$:
   $x = a_1$ x b_1 x $\frac{M}{p} + a_2$ x b_2 x $\frac{M}{q} =$
   4 x 2 x 11 + 1 x 8 x 7
   $x \equiv 144 = 67 \mod 77 \rightarrow \mathbf{x = 67}$
2) $x \equiv 3 \mod 7$ and $x \equiv 1 \mod 11$:
   $x = a_1$ x b_1 x $\frac{M}{p} + a_2$ x b_2 x $\frac{M}{q} =$
   3 x 2 x 11 + 1 x 8 x 7
   $x \equiv 122 = 45 \mod 77 \rightarrow \mathbf{x = 45}$
3) Now, we can take the advantage of symmetry to get the other two result:
   $7767 = 10 \rightarrow \mathbf{x = 10}$
   $7745 = 32 \rightarrow \mathbf{x = 32}$

Finally, the original message must be $\mathbf{10}, \mathbf{32}, \mathbf{45}$ or $\mathbf{67}$.

One way to be able to recognize which of all messages was the sent message is adding some information to the message, called redundant information.

3.4. Security of the Rabin Cryptosystem

Since the decryption function of the Rabin cryptosystem is based on computing square roots modulo N, it is logical to think that its security is based also on it. It is possible to prove that the hardness of breaking the Rabin cryptosystem is equivalent to the hardness of factoring, that is, computing square roots modulo a composite N is as hard as factoring N:

Proof: Let a factor oracle able to factor N. We know that a square has four roots, so there four elements in Z_N^* such that:

$$z_1^2 = z_2^2 = z_3^2 = z_4^2 = k \mod N$$

Now, an integer $z \in Z_N^*$ is chosen at random and $z^2 = y$ is computed. There are two possible cases: if y is a valid ciphertext. Using the factor oracle (N,y) we obtain one of four possible plaintext, x:

$$x \equiv \pm z \mod N \text{ or } x \equiv \pm wr \mod N$$

where w is one of the non-trivial square roots of 1 $\mod N$. In this case, is not possible to obtain the factorization of N. On the other hand, if y is not a valid ciphertext, we have:

$$x^2 \equiv z^2 \mod N \rightarrow x \not\equiv \pm z \mod N$$

In this case, the computation of $gcd(z + x, N)$ must yield p or q and the factorization N can be obtained.

Also, it is possible to compute the probability of success of this algorithm. For a residue $r \in Z_N^*$:

$$[r] = \{ \pm r \mod N, w \mod N \}$$

Any two reidues in $[r]$ yield the same value of y. The algorithm can obtain N if and only if $x \equiv \pm wr \mod N$, but the oracle doesn't know which of four possible values of r was chosen to construct y. So the probability that $x \equiv \pm w \mod N$ is $\frac{1}{2}$. □

4. Comparison with RSA Cryptosystem

The cryptosystems RSA and Rabin are very similar. Both are based on the hardness of factorization. The main difference is the fact that it is possible to prove that the problem of the Rabin cryptosystem is as hard as integer factorization, while hardness of solving the RSA problem is not possible to relate to the hardness of factoring, which makes the Rabin cryptosystem more secure in this way than the RSA.

Another difference is in the risk of attack. The Rabin cryptosystem is secure against a chosen plaintext attacks, however, the system can be broken using ciphertext attacks enabling the attacker to know the private key. RSA is also vulnerable to a chosen ciphertext attack, but the private key always remains unknown.

In terms of efficiency, the Rabin encryption process requires to compute roots modulo n more efficient than the RSA which requires the computation of n-th powers. About the decryption process both apply the the Chinese remainder theorem. The disadvantage in decryption process of Rabin system is that the process produces four results, three of them false results, while the RSA system just get the correct one.

5. Conclusion

The Rabin cryptosystem is an asymmetric cryptosystem where the private key is composed of two primes, p and q, and a public key composed of n=pq. It is based on the hardness of factoring. It is simple to compute square roots modulo a composite if the factorization is known, but very complex when the factorization is unknown.

The encryption process computes the square modulo n of the message, while the decryption process requires to compute modular square roots. Since the encryption process is not an injective function, four possible results will be obtained after applying the Chinese Remainder Theorem to solve the systems of congruences.

About the security, the Rabin cryptosystem is secure against a chosen plaintext attack because n=pq cannot be factored, however, is insecure against a chosen ciphertext attack.

Despite being a good alternative to the RSA cryptosystem, is not so popular like RSA, but the reasons are mainly just historical, not technical.

References

[1] Stinson, *Cryptography: Theory and Practice*, 2nd ed. Campman & Hall, 2001.

[2] Katz and Lindell, *Introduction to Modern Cryptography*, Ed. Campman & Hall, 2007

[3] http://scienceblogs.com/goodmath/2008/11/asymmetric_cryptography_the_b