The Rabin Cryptosystem & analysis in measure of Chinese Reminder Theorem

Arpit Kumar Srivastava[*], **Abhinav Mathur**[**]

[*] Department of Computer Science & Engineering, Galgotia's College of Engineering & Technology
[**] Department of Computer Science & Engineering, Galgotia's College of Engineering & Technology

Abstract- Cryptography is the practise and study of techniques for secure communication in the presence of third parties. The 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 analysed with the help of Chinese Reminder Theorem. Also, redundancy schemes for decryptions technique is mentioned and some basic mathematical concepts is explained and finally compared with RSA cryptosystem in terms of security and efficiency.

Index Terms- Rabin cryptosystem, Chinese Reminder Theorem, Jacobi symbol, Rabin signature scheme

I. Introduction

The Rabin cryptosystem is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. However the Rabin cryptosystem has the advantage that the problem on which it relies has been proved to be as hard as integer factorization, which is not currently known to be true of the RSA problem. It has the disadvantage that each output of the Rabin function can be generated by any of four possible inputs; if each output is a cipher text, extra complexity is required on decryption to identify which of the four possible inputs was the true plaintext.

The process was published in January 1979 by Michael O. Rabin. The Rabin cryptosystem was the first asymmetric cryptosystem where recovering the entire plaintext from the cipher text could be proven to be as hard as factoring.

II. Chinese Remainder theorem

Theorem: Suppose that m_1, m_2.., m_r are pairwise relatively prime positive integers, and let a_1, a_2... a_r be integers. Then the system of congruence's, $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$, has a unique solution modulo $M = m_1 \times m_2 \times ... \times m_r$, which is given by: $x \equiv a_1M_1y_1 + a_2M_2y_2 + ... + a_rM_ry_r \pmod{M}$, where $M_i = M/m_i$ and $y_i \equiv (M_i)^{-1} \pmod{m_i}$ for $1 \le i \le r$.

Pf: Notice that gcd $(M_i, mi) = 1$ for $1 \le i \le r$. Therefore, the y_i all exist (determined easily from the extended Euclidean Algorithm). Now, notice that since $Miyi \equiv 1 \pmod{m_i}$, we have $a_iM_iy_i \equiv a_i \pmod{m_i}$ for $1 \le i \le r$.

On the other hand, $a_iM_iy_i \equiv 0 \pmod{m_j}$ if $j \neq i$ (since $m_j \mid M_i$ in this case). Thus, we see that $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$.

If x0 and x1 were solutions, then we would have $x0 - x1 \equiv 0 \pmod{m_i}$ for all i, so $x0 - x1 \equiv 0 \pmod{M}$, i.e., they are the same modulo M.

III. Encryption

As with all asymmetric cryptosystems, the Rabin system uses both a public and a private key. The public key is necessary for later encryption and can be published, while the private key must be possessed only by the recipient of the message.

The precise key-generation process follows:

- Choose two large distinct primes *p* and *q*. One may choose $p \equiv q \equiv 3 \pmod{4}$ to simplify the computation of square roots modulo *p* and *q* (see below). But the scheme works with any primes.
- Let $n = p \cdot q$. Then *n* is the public key. The primes *p* and *q* are the private key.

To encrypt a message only the public key *n* is needed. To decrypt a cipher text the factors *p* and *q* of *n* are necessary.

For the encryption, only the public key *n* is used, thus producing a cipher text out of the plaintext. The process follows:

Let $P = \{0, ..., n-1\}$ be the plaintext space (consisting of numbers) and $m \in P$ be the plain text. Now the cipher text c is determined by

$c = m^2 \, mod \, n$

That is, *c* is the quadratic remainder of the square of the plaintext, modulo the key-number *n*.

IV. Decryption

To decode the cipher text, the private keys are necessary. The process follows:

If *c* and *r* are known, the plaintext is then $m \in \{0, ..., n-1\}$ with $m^2 \equiv c (mod \, r)$. For a composite *r* (that is, like the Rabin algorithm's $n = p \cdot q$) there is no efficient method known for the finding of *m*. If, however r is prime (as are *p* and *q* in the Rabin algorithm), the Chinese remainder theorem can be applied to solve for *m*.

Thus the square roots
$m_p = \sqrt{c} \, mod \, p$
And
$m_q = \sqrt{c} \, mod \, q$
Must be calculated

Now, by invocation of the Chinese remainder theorem, the four square roots $+r, -r, +s \text{ and } -s$ of $c + nZ \in Z/nZ$ are calculated (Z/nZ here stands for the ring of congruence classes modulo *n*). The four square roots are in the set $\{0, \ldots, n-1\}$

$$r = (y_p \cdot p \cdot m_p + y_q \cdot q \cdot m_p) \bmod n$$
$$-r = n - r$$
$$s = (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \bmod n$$
$$-s = n - s$$

One of these square roots $\bmod n$ is the original plaintext *m*. In our
Rabin pointed out in his paper, that if someone is able to compute both, $r \text{ and } s$, then he is also able to find the factorization of n because:
Either $gcd(|r-s, n|) = p \text{ or } gcd(|r-s, n|) = q$,

Where gcd means Greatest common divisor.

Since the Greatest common divisor can be calculated efficiently you are able to find the factorization of n efficiently if you know $r \text{ and } s.$

The decryption requires to compute square roots of the cipher text *c* modulo the primes *p* and *q*. Choosing $p \equiv q \equiv 3 \ (mod\ 4)$ allows to compute square roots by

$$m_p = c^{\left(\frac{p+1}{4}\right)} \bmod p$$

And

$$m_q = c^{\left(\frac{q+1}{4}\right)} \bmod q$$

We can show that this method works for *p* as follows. First $p \equiv 3 (mod\ 4)$ implies that (*p*+1)/4 is an integer. The assumption is trivial for *c*≡0 (mod *p*). Thus we may assume that *p* does not divide *c*. Then

$$m_p^2 \equiv c^{\left(\frac{p+1}{2}\right)} \equiv c \cdot c^{\left(\frac{p-1}{2}\right)} \equiv c \cdot \left(\frac{c}{p}\right) (mod\ p)$$

Where $\left(\frac{c}{p}\right)$ is a Legendre symbol. From $c = m^2 (mod\ pq)$ follows that $c = m^2 (mod\ p)$. Thus *c* is a quadratic residue modulo *p*. Hence $\left(\frac{c}{p}\right) = 1$ and therefore

$$m_p^2 \equiv c (mod\ p)$$

The relation $p \equiv 3 (mod\ 4)$ is not a requirement because square roots modulo other primes can be computed too.

Example: Let *n* = 77 = *pq* = 11 · 7 and *m* =32.

First, the message m must be encoded using the encryption function:

$e_k(32) = 32^2 \bmod 77 = 23 = c$

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:

$$m_p = c^{\left(\frac{p+1}{4}\right)} \bmod p \equiv 23^{\left(\frac{7+1}{4}\right)} \bmod 7 = 4$$
$$m_q = c^{\left(\frac{q+1}{4}\right)} \bmod q \equiv 23^{\left(\frac{11+1}{4}\right)} \bmod 11 = 1$$

And the system of congruence's $x \equiv a_i b_i \frac{M}{m_i}$ *is:*

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

Finally we can apply the Chinese remainder theorem to compute the four square roots:
First we compute b_1 and b_2 such:

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

Now, we can compute the solutions:

1) $x = 4 \bmod 7$ and $x = 1 \bmod 11$:

$$x = a_1 \times b_1 \times \frac{M}{p} + a_2 \times b_2 \times \frac{M}{q} = 4 \times 2 \times 11 + 1 \times 8 \times 7$$
$$x \equiv 144 \equiv 67 \bmod 77 \to x = 67$$

2) $x = 3 \bmod 7$ and $x = 1 \bmod 11$:

$$x = a_1 \times b_1 \times \frac{M}{p} + a_2 \times b_2 \times \frac{M}{q} = 3 \times 2 \times 11 + 1 \times 8 \times 7$$
$$x \equiv 122 \equiv 45 \bmod 77 \to x = 45$$

3) Now, we can take the advantage of symmetry to get the other two result:

$$7767 = 10 \to x = 10$$
$$7745 = 32 \to x = 32$$

Finally, the original message must be **10**, **32, 45** or **67**.

V. Redundancy Schemes for Unique Decryption

To ensure that decryption returns the correct message it is necessary to have some redundancy in the message, or else to send some extra bits. We now describe three solutions to this problem.

• **Redundancy in the message for Rabin**: For example, insist that the least significant *l* bits (where *l* > 2 is some known parameter) of the binary string m are all ones. If *l* is big enough then it is unlikely that two different choices of square root would have the right pattern in the *l* bits.

A message m is encoded as $x = 2^l\text{m} + (2^l - 1)$, and so the message space is $\text{M}_\kappa = \{\text{m}: 1 \leq \text{m} < N/2^l, \gcd(N, 2^l\text{m} + (2^l - 1)) = 1\}$ (alternatively, $\text{M}_\kappa = \{0,1\}^{\kappa-l-2}$). The cipher text is $\text{c} = x^2$ (mod *N*). Decryption involves computing the four square roots of c. If none, or more than one, of the roots has all *l* least significant bits equal to one and so corresponds to an element of M_κ then decryption fails (return ⊥). Otherwise output the message $\text{m} = \lfloor x/2^l \rfloor$.

• **Extra bits for Rabin**: Send two extra bits of information to specify the square root. For example, one could send the value $b_1 = \left(\frac{m}{N}\right)$) of the Jacobi symbol (the set {−1,1} can be encoded as a bit under the map $x \to 7\ (x+1)/2$), together with the least significant bit b_2 of the message. The cipher text space is now $\text{C}_\kappa = (Z/NZ)^* \times \{0,1\}^2$ and, for simplicity of exposition, we take $\text{M}_\kappa = (Z/NZ)^*$.

These two bits allow unique decryption, since $\left(\frac{-1}{N}\right) = 1$, m and *N* − m have the same Jacobi symbol, and if m is odd then *N* − m is even.

Indeed, when using the Chinese remainder theorem to compute square roots then one computes m_p and m_q such that $\left(\frac{m_p}{p}\right) = \left(\frac{m_q}{q}\right) = 1$. Then decryption using the bits b_1, b_2 is: if $b_1 = 1$ then the decryption is ±*CRT* (m_p, m_q) and if $b_1 = -1$ then solution is ±*CRT*($-\text{m}_p$, m_q).

This scheme is close to optimal in terms of cipher text expansion and decryption never fails. The drawbacks are that the cipher text contains some information about the message, and encryption involves computing the Jacobi symbol, which typically requires far more computational resources than the single squaring modulo N.

• **Williams**: Let $N = pq$ where $p,q \equiv 3 \pmod 4$. If p 6$\equiv \pm q \pmod 8$ then $(\frac{2}{N}) = -1$. Hence, for every $1 \leq x < N$ exactly one of x, $N - x$, $2x$, $N - 2x$ is a square modulo N. Without loss of generality we therefore assume that $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$. The integer N is called a **Williams integer** in this situation.

Williams [629] suggests encoding a message $1 \leq m < N/8 - 1$ (alternatively, $m \in M_\kappa = \{0,1\}^{\kappa-5}$) as an integer x such that x is even and $(\frac{x}{N}) = 1$ (and so x or $-x$ is a square modulo N) by

$$x = P(m) = \begin{cases} 4(2m+1) \; if \left(\frac{2m+1}{N}\right) = 1 \\ 2(2m+1) \; if \left(\frac{2m+1}{N}\right) = -1 \end{cases}$$

The encryption of m is then $c = P(m)^2 \pmod N$. One has $C_\kappa = (Z/NZ)^*$

To decrypt one computes square roots to obtain the unique even integer $1 < x < N$ such that $\left(\frac{x}{N}\right) = 1$ and $x^2 \equiv c \pmod N$. If $8 \mid x$ then decryption fails (return ⊥). Otherwise, return $m = (x/2 - 1)/2$ if $x \equiv 2 \pmod 4$ and $m = (x/4 - 1)/2$ if $x \equiv 0 \pmod 4$.

Unlike the extra bits scheme, this does not reveal information about the cipher text. It is almost optimal from the point of view of cipher text expansion. But it still requires the encrypter to compute a Jacobi symbol (hence losing the performance advantage of Rabin over RSA). The Rabin cryptosystem with the Williams padding is sometimes called the **Rabin-Williams cryptosystem**.

VI. Rabin Signature Scheme

The Rabin signature scheme is a variant of the RSA signature scheme. It has the advantage over RSA that finding the private and forgery key are both as hard as factoring. In Rabin scheme, public key is an integer n where $n = p \cdot q$ and p and q are prime numbers which form the private key. The message which is to be signed must have a square root mod n otherwise, it has to be modified slightly. Only about ¼ of all possible message have square root mod n.

• **Signature**: $s = m^{\frac{1}{2}} \; mod \, n$ where s is the signature
• **Verification**: $m = s^2 \; mod \, n$

The signature is easy to compute if the prime factors of n are known, but probably difficult otherwise- anyone who can forge the signature can also find factor n. The provable security has the side-effect that the prime factor can be recovered under a chosen message attack. This attack can be countered by padding a given message with random bits or modifying the message randomly, at the loss of provable security.

VII. 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 cipher text attacks enabling the attacker to know the private key. RSA is also vulnerable to a chosen cipher text 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 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.

VIII. Conclusion

This Rabin cryptosystem is an asymmetric cryptosystem where the private key is composed of two primes, p and q, and a public key composed of $n = p \cdot q$. 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.

In terms of computational performance, Rabin encryption is extremely fast (as long as encryption does not require computing a Jacobi symbol) while decryption, using the Chinese remainder theorem, is roughly the same speed as RSA decryption.

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 congruence’s.

Difference between Rabin cryptosystem and RSA cryptosystem is clearly mentioned in reference of mode of attacks, security issues and their efficiency.

This paper give a general idea about Rabin cryptosystem and its encryption and decryption procedure are shown with help of few theorem of Chinese Remainder Theorem along with suitable example.

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] Bucher Gruppe, Asymmetrisches Verschlusselungsverfahren: Rsa-Kryptosystem, Asymmetrisches Kryptosystem, Rabin-Kryptosystem, Elgamal-Kryptosyste

[4] Paul van Oorschot, A. J. Menezes, Scott Vanstone, Alfred Menezes, *Handbook on Applied Cryptography*

[5] http://scienceblogs.com/goodmath/2008/11/asymmetric cryptography the basic

[6] http://en.wikipedia.org/wiki/Rabin_cryptosystem#Evaluation_of_the_algorithm

[7] http://www.math.auckland.ac.nz/~sgal018/crypto-book/ch25.pdf

[8] http://www.cs.uni-paderborn.de/fileadmin/Informatik/AG-Bloemer/lehre/2011/ss/seminar/Naiara_Sanchez_-_Rabin_Cryptosystem.pdf

[9] http://www-math.ucdenver.edu/~wcherowi/courses/m5410/crt.pdf

[10] Wenbo Mao, Modern Cryptography theory and practises

AUTHORS

First Author – Arpit Kumar Srivastava, Student, Galgotias College of Engineering & Technology, arpityuuvraaj@gmail.com.
Second Author – Abhinav Mathur, Student, Galgotias College of Engineering & Technology, abhinav23mat@gmail.com