International Journal of Information & Network Security (IJINS)
Vol.4, No.1, February 2015, pp. 11~13
ISSN: 2089-3299

Rabin Cryptosystem and Its Extension

Nisheeth Saxena*, Dr.Rajeev Pourush**
* Assistant Professor – CSE Department - FET MUST
** Assistant Professor – ECE Department – FET MUST

Article Info

Article history:

Received Dec 12th, 2014
Revised Jan 20th, 2015
Accepted Feb 26th, 2015

Keyword:

Rabin cryptosystem,
cipher text,
integer factorization

ABSTRACT

The Rabin cryptosystem is an asymmetric cryptographic algorithm. Its security is based on the problem of integer factorization [4]. Rabin cryptosystem has the advantage that the problem on which its security depends is proved to be as hard as factorization [5]. Its minor disadvantage is that each output of the Rabin algorithm is 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 [2]. 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 integer factorization.

Corresponding Author:

Nisheeth Saxena,
Assistant Professor – CSE Department - FET MUST,
Email: nisheethsaxena.fet@mitsuniversity.ac.in, *rajeevpourush.fet@modyuniversity.ac.in*

1. INTRODUCTION

The Rabin cryptosystem is a variation of the RSA cryptosystem. Rabin cryptosystem is based on the concept of quadratic congruences while RSA cryptosystem is based on exponentiation congruences [4].In Rabin cryptosystem value of e and d are fixed and are equal to 2 and ½ respectively. In RSA cryptosystem 1<e< ∅ (n) and e is coprime to ∅(n) , whereas d is inverse of e modulo ∅(n) i.e. $d = e^{-1}\ mod\ \emptyset(n)$[4].The equations for encryption and decryption can be written as :

$C \equiv P^2\ (mod\ n)$ $\quad$ $P \equiv C^{\frac{1}{2}}(mod\ n)$

The public key in the Rabin Cryptosystem is given by $n = p * q$, where p and q are very large prime numbers and the 2-tuple (p, q) forms the private key. Everyone can encrypt the a message using n but only intended recipient (Bob)can decrypt the message using $p\ and\ q$.Bob needs to keep $p\ and\ q$ untill the end of the decryption process, he can't discard them after the key generation procedure is over.

The two primes selected for key generation can be congruent to $3\ mod\ 4$ as well as $1\ mod\ 4$. The decryption process is easier when $p\ and\ q$ are of the form $p\ and\ q \equiv 3(\text{ mod } 4)$. The decryption process is much more difficult when we take $p\ and\ q$ of the form $p\ and\ q \equiv 1(\text{ mod } 4)$. The Rabin cryptosystem is implemented only for the primes of the form $p\ and\ q \equiv 3(\text{ mod } 4)$. We will extend Rabin cryptosystem for the class of integers which are congruent to $5\ mod\ 8$, which can be considered as a subset of the set of primes belonging to the set $1\ mod\ 4$.

Algorithm Rabin_Key_Generation {
// Choose two large prime numbers $p\ and\ q$ of the form $4k + 3$ i.e. both are congruent to $3\ mod\ 4\ and\ p \neq q$.
$n = p * q$;
Public_Key = n ;
Private_Key = (p, q);
Send(Public_Key , Private_Key) ;

}

Lemma 1: Let p be a prime satisfying $p \equiv 3\ (mod\ 4)$ and suppose that a is a quadratic residue modulo . Then $x = \pm a^{(p+1)/4}$ is a solution to the congruence: $x^2 \equiv a\ (mod\ p\ )$[3]
Lemma 2: Let p be a prime satisfying $p \equiv 5\ (mod\ 8)$ and suppose that a is a quadratic residue modulo . Then one of the values $x = a^{(p+3)/8}\ or\ x = 2a.(4a)^{(p-5)/8}$ is a solution to the congruence: $x^2 \equiv a\ (mod\ p\ )$[3].
Proof: The above two lemmas have straightforward proof.
We denote the two plaintexts obtained after decryption as$P_1\ and\ P_2$. Whereas the plaintext selected before encryption is P.

There are two cases for the selection of plaintext.

(1) $P < p$ If the value of the plaintext is less than , the prime number selected.
In this case solution is obtained directly by either $P_1\ or\ P_2$.

(2) $P \geq p$ If the value of the plaintext is greater than or equal to , the prime number selected.

In this case solution is obtained $by\ the\ value\ of\ pk - P_1\ \ or\ pk - P_2\ where\ k = 1,2,3, \ldots$

Example 1 (Case 1) : Let $p = 29$ and $q = 13$ (both are congruent to 5 mod 8)
Now Bob calculates $n = p * q = 29 * 13 = 377$, n is announced publicly by Bob and he keeps $p\ and\ q$ as secret.Alice wants to send the plaintext $P = 24$, here 377 and 24 are relatively prime and 24 is in Z_{377}^*.The set Z_n^* is a subset of Z_n , and it includes only those integers in Z_n which have a unique multiplicative inverses.Also here value of plaintext (P) is less than p. Alice calculates the cipher text as : $C = 24^2\ (mod\ 377) = 199\ (mod\ 377)$. She sends the cipher text 199 to Bob.
Bob receives the cipher text $C = 199\ , which\ is\ actually\ a\ here$, and calculates the values of plain texts $P_1\ or\ P_2$ as follows:
$P_1 = a^{(p+3)/8}(mod\ p)$ or $P_2 = 2a.(4.a)^{(p-5)/8}\ (mod\ p)$
Here $P_1 = 199^{(29+3)/8}\ (mod\ 29) = 24\ (mod\ 29)$.
Or $P_2 = (2 * 199).(4 * 199)^{(29-5)/8}(mod\ 29\ ) = 27$.
Out of the two possible answers Bob takes the first one. The selection of the answer is done by Bob, based on the situation.

Example 2 (Case 2) : Let $p = 37$ and $q = 29$ (both are congruent to 5 mod 8)
Now Bob calculates $n = p * q = 37 * 29 = 1073$, n is announced publicly by Bob and he keeps $p\ and\ q$ as secret.Alice wants to send the plaintext $P = 65$, here 1073 and 65 are relatively prime and 65 is in Z_{1073}^*.Here value of plaintext (P) is greater than p. Alice calculates the cipher text as : $C = P^2(mod\ n\ )$
$C = 65^2\ (mod\ 1073) = 1006\ (mod\ 1073)$. She sends the cipher text 1006 to Bob.
Bob receives the cipher text $C = 1006\ , which\ is\ actually\ 'a'\ here$, and calculates the values of plain texts $P_1\ or\ P_2$ as follows:
$P_1 = 1006^{(37+3)/8}\ (mod\ 37) = 9\ (mod\ 37)$.
Or $P_2 = (2 * 1006).(4 * 1006)^{(37-5)/8}(mod\ 37\ ) = 20$.
Here selection of plaintext depends upon the value of $pk - P_1\ where\ k = 1,2,3, \ldots$
Therefore the solution is: $(37 * 2 - 9) = 65\ , k = 2\ , p = 37\ , P_1 = 9$.
After decryption Bob takes the plaintext as : 65 , which is the desired value.

Example 3 (Case 1): Let $p = 37$ and $q = 29$ (both are congruent to 5 mod 8)
Now Bob calculates $n = p * q = 37 * 29 = 1073$, n is announced publicly by Bob and he keeps $p\ and\ q$ as secret.Alice wants to send the plaintext $P = 10$, here 1073 and 10 are relatively prime and 10 is in Z_{1073}^*.Here value of plaintext (P) is less than p. Alice calculates the cipher text as :
$C = 10^2\ (mod\ 1073) = 100\ (mod\ 1073)$. She sends the cipher text 100 to Bob.
Bob receives the cipher text $C = 100\ , which\ is\ actually\ 'a'\ here$, and calculates the values of plain texts $P_1\ or\ P_2$ as follows:
$P_1 = 100^{(37+3)/8}\ (mod\ 37) = 10\ (mod\ 37)$.
Or $P_2 = (2 * 100).(4 * 100)^{(37-5)/8}(mod\ 37\ ) = 14$.
After decryption Bob takes the plaintext $P_1 = 10$, which is the desired value.

Example 4 (Case 2) : Let $p = 37$ and $q = 29$ (both are congruent to 5 mod 8)
Now Bob calculates $n = p * q = 37 * 29 = 1073$, n is announced publicly by Bob and he keeps $p\ and\ q$ as secret.Alice wants to send the
plaintext $P = 40$, here 1073 and 40 are relatively prime and 40 is in Z^*_{1073}.Here value of plaintext (P) is greater than p. Alice calculates the cipher text as :
$C = 40^2\ (mod\ 1073) = 527\ (mod\ 1073)$. She sends the cipher text 527 to Bob.
Bob receives the cipher text $C = 527$, $which\ is\ actually\ 'a'\ here$, and calculates the values of plain texts $P_1\ or\ P_2$ as follows:
$P_1 = 527^{(37+3)/8}\ (mod\ 37) = 34\ (mod\ 37)$.
Or $P_2 = (2 * 527).(4 * 527)^{(37-5)/8} (mod\ 37)$.
Here selection of plaintext depends upon the value of $pk - P_1\ where\ k = 1,2,3, \ldots$
Therefore the solution is: $(37 * 2 - 34) = 40$, $k = 2$, $p = 37$, $P_1 = 34$.
After decryption Bob takes the plaintext as: 40 , which is the desired value.

2. SECURITY

The great advantage of the Rabin cryptosystem is that a random plaintext can be recovered entirely from the ciphertext only if the codebreaker is capable of efficiently factoring the public key *n*. Note that this is a very weak level of security. Extensions of the Rabin cryptosystem achieve stronger notions of security [1].

It has been proven that decoding the Rabin cryptosystem is equivalent to the integer factorization problem, which is rather different than for RSA. Thus the Rabin system is 'more secure' in this sense than is RSA, and will remain so until a general solution for the factorization problem is discovered, or until the RSA problem is discovered to be equivalent to factorization. (This assumes that the plaintext was not created with a specific structure to ease decoding)[2].

Since the solution to the factorization problem is being sought on many different fronts, any solution (outside classified research organizations such as NSA) would rapidly become available to the whole scientific community. However, a solution has been long in coming, and the factorization problem has been, thus, practically insoluble. Without such an advance, an attacker would have no chance today of breaking the code. This cryptosystem is provably secure (in a strong sense) against chosen plaintext attacks. However, an active attacker can break the system using a chosen ciphertext attack, as has been mathematically proven.

REFERENCES

[1]C.C.Chang & C.H.Lin “An ID based signature scheme based upon Rabin public key cryptosystem” IEEE 1991.
[2]Ming Yung Ko , T.Hwang and C.C.Chang “Attacks on ID based signature scheme based upon Rabin’s public key cryptosystem” IEEE 1993.
[3]Josef H. Silverman , “A friendly introduction to number theory” , Pearson education , 3rd edition -2009.
[4]Behrouz A. Forouzan, Debdeep Mukhopadhyay , “Cryptography and Network Security” , Tata McGraw Hill education Private Limited – New Delhi , Second edition, 2011.
[5]William Stallings, “Cryptography and Network Security Principles and Practice”, Pearson, Fifth Edition 2011.