*Mody University International Journal of Computing and Engineering Research*
*Vol. 1 Issue 1, 2017, pp.7-10*
*ISSN: 2456-9607 (Print) 2456-8333(Online)*

# On the Extension of the Domain of Rabin Cryptosystem

**Nisheeth Saxena**

*Department of Computer Science and Engineering,*
*Mody University of Science and Technology, Lakshmangarh, India*

*nisheeth.somnath@gmail.com*

*Received 15 Nov. 2016, Published 31 March. 2017*

**Abstract:** The Rabin cryptosystem is an asymmetric cryptographic algorithm. Its security is based on the problem of integer factorization. Rabin cryptosystem has the advantage that the problem on which its security depends is proved to be as hard as factorization. The Rabin cryptosystem works in the domain of the odd primes which satisfy the criteria that $p \equiv 3\ (mod\ 4)$, where $p$ is any odd prime. The decryption process is very difficult when we take the odd primes which satisfy $p \equiv 1\ (mod\ 4)$. Rabin cryptosystem will be more applicable and flexible if we include a wide range of primes. We have extended the domain of primes in Rabin cryptosystem to a subset of the primes satisfying $p \equiv 5\ (mod\ 8)$. The primes satisfying $p \equiv 5\ (mod\ 8)$ forms a subset of the primes satisfying $p \equiv 1\ (mod\ 4)$ without compromising on the security of the Rabin cryptosystem. Our proposed method covers a larger range of primes for the Rabin cryptosystem as compared to original method. Our method is especially useful for resource constrained Networks such as Mobile Ad Hoc Networks (MANET).

**Keywords:** *Rabin cryptosystem, cipher text, integer factorization, Mobile Ad Hoc Networks (MANET)*

## 1. INTRODUCTION

The Rabin cryptosystem is a variation of the RSA cryptosystem. Rabin cryptosystem is based on the concept of quadratic congruence's while RSA cryptosystem is based on exponentiation congruence [1].

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][3]. 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 [7][8][9][10].

The paper is organized as follows:

In section 2 we have given mathematical background for Rabin cryptosystem. In section 3 we discuss proposed method along with the lemmas and their proofs in support of our method. Section 4 gives some toy examples for the clarification of our proposed method. Section 5 discusses the security of our method and section 6 concludes the paper.

## 2. MATHEMATICAL BACKGROUND

In Rabin cryptosystem value of e and d are fixed and are equal to 2 and ½ respectively. In RSA cryptosystem 2<e<∅ (n) and e is co-prime 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 :

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

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 $1\ mod\ 4$.

## 3. PROPOSED METHOD

All odd primes can be divided into two categories the primes which are congruent to 1 (mod 4) and the primes which are congruent to 3 (mod 4) represented by the sets namely$S_1\ and\ S_2$ respectively where:
$S_1 = \{\mathbf{5}, \mathbf{13}, 17, \mathbf{29}, \mathbf{37}, 41, \mathbf{53} \ldots\}\ and\ S_2 =$ { 3,7,11,19,23,31,43 …}. Rabin Cryptosystem

addresses the primes of set $S_2$ while our proposed method deals with the set $S_3 \subset S_1$. The elements of set $S_3$ *are* represented in bold italic in set $S_1, i.e. S_3 = \{5,13,29,37,53, \ldots\ldots\}$ , the primes congruent to 5 (mod 8) .

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) ;
}

Our method is based upon the application of following two lemmas.

**3.1 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: $x^2 \equiv a\ (mod\ p\ )$.

Proof: Given $p \equiv 3\ (mod\ 4)$ and $x = \pm a^{\left(\frac{p+1}{4}\right)}$

$\Rightarrow x^2 = a^{(p+1)/2} = a^{(p+2-1)/2} = a^{(p-1)/2}.a$

Let$A = a^{(p-1)/2} \implies A^2 = a^{(p-1)} \equiv 1\ (mod\ p)$ by Fermat's little theorem.

Hence $p|(A^2-1) \implies p|(A+1)(A-1)$

Since $p$ is an odd prime, it divides either$(A+1) or\ (A-1)$.

Thus $A$ must be congruent to $+1\ or\ -1$, actually $A \equiv 1\ (mod\ p)$, when $a$ is a quadratic residue$(mod\ p)$, and $A \equiv -1\ (mod\ p)$ when $a$ is a quadratic non residue $(mod\ p)$.This is according to Euler's criterion [3] which says that:

If $p$ is an odd prime then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\ mod\ p\ where\ \left(\frac{a}{p}\right)$ represents value of the Legendre symbol.

**3.2 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:

$$x^2 \equiv a\ (mod\ p\ ).$$

**Proof:**

When $x = a^{(p+3)/8} \implies x^2 = a^{(p+3)/4}$

Since $p \equiv 5\ (mod\ 8)$ , $p = 8*k+5\ for\ k = 0,1,2, \ldots$

$x^2 = a^{(8*k+8)/4} \implies x^2 = a^{2*k}.a^2$, where a is a quadratic residue - mod p

It means $x^2 = a\ (mod\ p)$ , since multiplication of two quadratic residues is again a quadratic residue.

Similarly another part of the lemma can also be proved.

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 $by\ the\ value\ of\ pk - P_1\ \ or\ pk - P_2\ where\ k = 1,2,3, \ldots$

## 4. SOME TOY EXAMPLES

**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 $Z^*_n$ *i*s 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

$P_2 = (2*199).(4*199)^{\frac{29-5}{8}}(mod\ 29) = 27.$

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.

## 5. SECURITY

Rabin Cryptosystem's security is based on the difficulty of solving the factorization problem [3]. This is just like RSA where an adversary tries to attack the modulus n to find its two prime factors p and q. Our proposed method adds stronger notions of security for Rabin Cryptosystem [4].
It has been proven that breaking the Rabin cryptosystem is equivalent to the integer factorization problem. We can consider Rabin cryptosystem to be 'more secure' than RSA, since its security is based on Factorization as well as solving Quadratic residues equations. In our proposed method we assume that plaintext was not created with a specific structure to ease decryption [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.
Although Factorization is not proved to be NP - complete, but it is supposed to be intrinsically hard to crack. However, an efficient solution has not been discovered yet so it is considered practically insolvable. Without a dramatic advancement, an attacker would have no chance today of breaking the cryptosystems based on Factorization. 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.

## 6. CONCLUSION

In this paper we have enhanced the domain of prime numbers over which original Rabin cryptosystem is based on. Our method gives a slight extension to Rabin cryptosystem. This extended version of Rabin cryptosystem may prove useful for resource constrained Mobile Ad Hoc Networks (MANET). We have given several toy examples to support our argument.

In terms of efficiency Rabin and RSA cryptosystems are similar. Our proposed method is also as secure as RSA or existing Rabin cryptosystem but having a larger domain for the choice of prime numbers. If we use a large exponent e , then computing eth power in RSA is slower than the squaring in case of Rabin Cryptosystem[6][7][8].Therefore Rabin cryptosystem

is advantageous to use in resource constrained networks such as MANET.Our proposed method adds more flexibility and ease of use for existing Rabin Cryptosystem. Rabin cryptosystem works over a subset of $Z_{N^*}$ , our proposed method works over a larger subset of $Z_{N^*}$ , in contrast to RSA which gives a permutation over all $Z_{N^*}$[7].

## REFERENCES

[1] Behrouz A. Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", Tata McGraw Hill education private limited – New Delhi, second edition, 2011.

[2] Ming Yung Ko, T. Hwang and C.C. Chang "Attacks on ID based signature scheme based upon Rabin's public key cryptosystem" in IEEE International Carnahan Conference on Security Technology, 1993.

[3] Michele Elia, MatteoPiya, David Eschipani,"The Rabin Cryptosystem Revisited", Applied Algebra in Engineering, Communication and Computing, Volume 26 Issue 3, 2015, pp 251-275.

[4] Josef H. Silverman, "A friendly introduction to number theory", Pearson education, 3rd edition , 2009.

[5] C.C.Chang & C.H.Lin "An ID based signature scheme based upon Rabin public key cryptosystem" IEEE 1991.

[6]William Stallings, "Cryptography and Network Security Principles and Practice", Pearson, Fifth Edition, 2011.

[7] Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography", CRC Press, second edition, 2016.

[8] D.R.Stinson,"Cryptography Theory and Practice"CRC Press, Third Edition, 2013.

[9] Wade Trappe, Lawrence C. Washington," Introduction to Cryptography with Coding Theory", Pearson Education, second edition, 2012.

[10] Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2015 reprint.