Journal of Mathematics and Statistics 10 (3): 304-308, 2014
ISSN: 1549-3644

doi:10.3844/jmssp.2014.304.308 Published Online 10 (3) 2014 (http://www.thescipub.com/jmss.toc)

H-RABIN CRYPTOSYSTEM

Hayder Raheem Hashim

Department of Mathematics,
Faculty of Mathematics and Computer Science, University of Kufa, Najaf, Iraq

Received 2013-04-12; Revised 2013-07-16; Accepted 2014-05-15

ABSTRACT

Cryptography is the science of using mathematics that's used to hide information or data that is being sent between participants in a way that prevents other people from reading it. The need of exchanging messages secretly promoted the creation of cryptosystems to enable receivers to interpret the exchanged information. In this study, a particular public key cryptosystem called Rabin Cryptosystem is presented considered with the help of Chinese Reminder Theorem. Since the decryption algorithm of the Rabin cryptosystem is based on computing square roots modulo n, where n = p.q where p and q are primes. This study suggests a modification of Rabin cryptosystem that can make the cryptosystem more immune against some attacks. This modification focuses on considering n = p.q.r where p, q and r are primes. This new modification of Rabin cryptosystem is called H-Rabin Cryptosystem. Also, some basic mathematical concepts are explained and it finally compares the H-Rabin Cryptosystem, RSA cryptosystem and Rabin cryptosystem in terms of security and efficiency. This H-Rabin cryptosystem is a public key cryptosystem where the private key is composed of three primes, p, q and r and a public key composed of n = p.q.r and it is based on the hardness of factoring. Therefore, this new modification can make the cryptosystem more immune against some future attacks.

Keywords: Cryptography, Rabin Cryptosystem, Chinese Reminder Theorem, H-Rabin Cryptosystem, RSA Cryptosystem

1. INTRODUCTION

The Rabin cryptosystem is a public key cryptosystem technique, whose security, like that of RSA cryptosystem, is related to the difficulty of integer factorization (Haraty *et al*., 2006). This cryptosystem was suggested in 1979 by Michael Rabin as a variant of RSA cryptosystem for which factorization of modulo n has almost the same computational complexity as obtaining the decryption transformation from the encryption transformation (Rosen, 2005). The advantage of Rabin cryptosystem is that it has been proven that the decryption of Rabin cryptosystem is as difficult as the integer factorization, which is not currently known to be true of the RSA problem (WFE, 2014). The disadvantage of it is that each output of the Rabin algorithm can be generated by four possible inputs. So, each output, which is a block of a cipher text, is presented in the decryption procedure to four possible inputs which represent a block of the original plaintext.

2. CHINESE REMAINDER THEOREM

2.1. Theorem

Let $m1$, $m2$.., mr are pairwise relatively prime positive integers and let $a1$, $a2$... ar be integers. Then the system of congruence's, $x \equiv ai \pmod{mi}$ for $1 \le i \le r$, has a unique solution modulo M. (Sorin, 2007) Where, $M = m_1.m_2...m_r$, which is given by:

$$x \equiv a1M1y1 + a2M2y2 + ... + arMryr \pmod{M},$$
$$\text{where } Mi = M / mi = m_1.m_2....m_{i-1}.m_{i+1}.mr \text{ and}$$
$$yi \equiv (Mi)^{-1} \pmod{mi} \text{ for } 1 \le i \le r$$

2.2. Proof

It is clear that, gcd (Mi, mi) = 1 for $1 \le i \le r$ and gcd(mi, mj) = 1 whenever $i \ne j$. Therefore, the yi all exist (determined easily from the extended Euclidean

Algorithm). We can find an inverse yi of *Mi*, so that *Miyi* ≡ 1 (*mod mi*), we have aiMiyi ≡ ai (mod mi) for 1≤*i*≤r. On the other hand, *aiMiyi* ≡ 0 (*mod mj*) if *j* ≠ *i* (since *mj* | Mi in this case). Thus, we see that *x* ≡ *ai* (mod mi) for 1≤*i*≤*r* (Arpit and Mathur, 2013).

If *x*0 and *x*1 were solutions, then we would have *x*0-*x*1 ≡ 0 (*mod mi*) for all *i*, so *x*0-*x*1 ≡ 0 (*mod M*), Therefore *x*1 ≡ *x*0 (*mod M*). This shows that the solution the system of *r* congruences is unique modulo *M*.

3. ENCRYPTION OF RABIN CRYPTOSYSTEM

All the public key cryptosystems have a public and a private key. The public key is used in the encryption procedure and can be published, while the private key must be possessed only by the recipient of the message and used in the decryption procedure (Jeffrey *et al*., 2008).

The key-generation process is as the following:

- Choose two large distinct primes *p* and *q*. However the scheme works with any primes, choose *p* ≡ *q* ≡ 3 (mod 4) to simplify the computation of square roots modulo *p* and *q* (see below) (Arpit and Mathur, 2013)
- Let *n* the public key such that n = p.q
- Let the primes *p* and *q* are the private key

To encrypt a message only the public key *n* is needed, thus a cipher text is produced out of the original plaintext. To decrypt a cipher text the factors *p* and *q* of *n* are needed.

The encryption process is as the following:

- Let P = {0, 1, 2,……,n-1} be the plaintext space (consisting of numbers)
- Let m∈P = {0, 1, 2,……,n-1} be the plaintext
- Let C be the cipher text that can be computed by, C ≡ m^2 (mod n)

Now the encoded message can be sent as C. Once the message reaches the destination, it must be decrypted (Rabin, 2014).

4. DECRYPTIONOF RABIN CRYPTOSYSTEM

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

If *C* and *t* are known, the plaintext is m∈P with C ≡ m^2 (mod n). For a composite *t* (that is, like the Rabin algorithm's n = p.q) there is no efficient method known for the finding of *m*. If, however t is prime (as are *p* and *q* in the Rabin algorithm), the Chinese remainder theorem can be applied to solve for *m* (Arpit and Mathur, 2013).

Therefore the square roots:

$$m_p = \sqrt{c} \bmod p \quad m_q = \sqrt{c} \bmod q$$

Have to be computed.

So, by the supplication of the Chinese remainder theorem, four square roots come out. The four square roots are t, -t, +s and-s of $c + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ are Computed ($\mathbb{Z}/n\mathbb{Z}$ here stands for the ring of congruence classes modulo *n*). The four square roots are in the set {0, 1, 2,……,*n*-1}:

- t ≡ (y_p.p.m_q + y_q.q.m_p)(mod n)
- -t ≡ n-t
- S ≡ (y_p.p.m_q-y_q.q.m_p)(mod n)
- -s ≡ n-s

One of these square roots (mod n) is the original plaintext *m*. Rabin pointed out in his study, that if someone is able to compute both, r and S, then he is also able to find the factorization of because.

Either gcd (|t-s|,n) = p or gcd (|t-s|,n) = q, where gcd means the 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 t and s.

The decryption procedure requires to compute square roots of the cipher text *C* modulo the primes *p* and *q* (Schmidt-Samoa, 2006). Picking *p* ≡ *q* ≡ 3 (mod 4) permits to calculate square roots by:

$$m_p = C^{\frac{1}{4}(p+1)} \bmod p$$

And:

$$m_q = C^{\frac{1}{4}(q+1)} \bmod q \ .$$

We can show that this method works for *p* as the following: -Let p ≡ 3 (mod 4) implies that (*p*+1)/4 is an integer, by using the definition of modulo. The assumption is trivial for *c* ≡ 0 (mod *p*). Thus we may assume that *p* does not divide *c*. Then:

$$m_p^2 \equiv C^{\frac{1}{4}(p+1)} \equiv C.C^{\frac{1}{4}(p-1)} \equiv c.\left(\frac{c}{p}\right)(\text{mod } p)$$

where, $\frac{c}{p}$ is a Legendre symbol.

Fromc ≡ m^2 (mod p.q) implies that c≡m^2 (mod p.q). Thus *c* is a quadratic residue modulo *p*, so $\frac{c}{p}$ =1.

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 becomputed too. e.g., Rabin proposes to find the square roots modulo primes by using a special case of Berlekamp's algorithm (Arpit and Mathur, 2013).

5. H-RABIN CRYPTOSYSTEM

H-Rabin cryptosystem is a suggesting cryptosystem that suggest a modification of Rabin cryptosystem that can make the cryptosystem more immune against some attacks. This modification focuses on considering n = p.q.r where p, q and r are primes. This new modification of Rabin cryptosystem is called H-Rabin Cryptosystem.

6. ENCRYPTION OF H-RABIN CRYPTOSYSTEM

The key-generation process of H-Rabin crypto system is as the following:

- Choose three large distinct primes *p*, *q and r*. However the scheme works with any primes, choose p ≡ q ≡ r ≡ 3 (mod 4) to simplify the computation of square roots modulo *p*, *q* and r
- Let *n* the public key such that n = p.q.r
- Let the primes *p*, *q* and r are the private key

To encrypt a message only the public key *n* is needed, thus a cipher text is produced out of the original plaintext. To decrypt a cipher text the factors *p*, *q and r* of *n* are needed.

The encryption process of H-Rabin cryptosystem is as the following:

- Let P = {0, 1, 2,……,n-1} be the plaintext space (consisting of numbers)
- Let m ∈ P = {0, 1, 2,……,n-1} be the plaintext
- Let C be the cipher text that can be computed by, C = e_k(m) ≡ m^2 (mod n)

Now the encoded message can be sent as C. Once the message reaches the destination, it must be decrypted.

7. DECRYPTION OF H-RABIN CRYPTOSYSTEM

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

- Use the decryption function, $d_K(c) \equiv \sqrt{c}$ (mod n)
- Since the encryption function e_K is not an injection function, the decryption is not ambiguous. There exist eight square roots of c mod n (c = m^2 mod n), so there are eight possible messages, m (Rabin, 2014)
- The decryption try to determine m such that: C ≡ m^2 (mod n)
- This is equivalent to solving the three congruences:

$$z^2 \equiv c\ (mod\ p)$$
$$z^2 \equiv c\ (mod\ q)$$
$$z^2 \equiv c\ (mod\ r)$$

Then:

$$m_p \equiv (c)^{\frac{p+1}{4}} (\text{mod } p)$$
$$m_q \equiv (c)^{\frac{q+1}{4}} (\text{mod } q)$$
$$mr \equiv (c)^{\frac{r+1}{4}} (\text{mod } r)$$

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

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

Example

Let n = 1463 = p.q.r = 7. 11.19 and m = 41. First, the message m must be encrypted using the encryption function:

$$C = e_k(m) \equiv m^2\ (mod\ n)$$
$$C = e_K(41) \equiv 41^2 (mod 1463 \equiv 218$$

The encrypted message C = 218 is sent to the receiver. The receiver must decrypt the message C and has to find the eight square roots of 218 modulo 7, modulo 11 and modulo 19. The decryption algorithm is applied:

$$m_p \equiv (C)^{\frac{p+1}{4}} (mod\ p) \equiv (218)^{\frac{7+1}{4}} (mod\ 7) \equiv 1$$
$$m_q \equiv (C)^{\frac{q+1}{4}} (mod\ q) \equiv (218)^{\frac{11+1}{4}} (mod\ 11) \equiv 3$$
$$m_r \equiv (C)^{\frac{r+1}{4}} (mod\ r) \equiv (218)^{\frac{19+1}{4}} (mod\ 19) \equiv 16$$

The system of congruences, $x \equiv aibi\frac{M}{mi}$ is:

$$+m_p(\ mod\ p) \equiv 1(mod\ 7)$$
$$-m_p(mod\ p) \equiv 6(mod\ 7)$$
$$+m_q(mod\ q) \equiv 3(mod\ 11)$$
$$-m_q(mod\ q) \equiv 8(mod\ 11)$$
$$+m_r(mod\ r) \equiv 16(mod\ 19)$$
$$-m_r(mod\ r) \equiv 3(mod\ 19)$$

Finally, we can apply the Chinese remainder theorem to compute the eight roots:

First of all, we compute b_1, b_2 and b_3 such:

- $\frac{N}{7}$ $b_1 \equiv 1$ (mod 7)→ 209 $b_1 \equiv 1$ (mod 7)→ 6 $b_1 \equiv 1$ (mod 7) → $b_1 = 6$
- $\frac{N}{11}$ $b_2 \equiv 1$ (mod 11)→ 133 $b_2 \equiv 1$ (mod 11)→ $b_1 \equiv 1$ (mod 11) → $b_2 = 1$
- $\frac{N}{19}$ $b_3 \equiv 1$ (mod 19)→ 77 $b_3 \equiv 1$ (mod 19)→ $b_3 \equiv 1$ (mod 19) → $b_3 = 1$

We can compute the following solutions:

- X ≡ 1 (mod 7), x ≡ 3 (mod 11) and x ≡ 16 (mod 19): $x \equiv a^1b_1\frac{M}{p} + a_2b_2\frac{M}{q} + a_3b_3\frac{M}{r}$ (mod n) x ≡ [(1)(6)(11.19) + (3)(1)(7.19) + (16)(1)(7.11)] (mod 1463) x ≡ 2885 (1463)→ x = 1422
- X ≡ 6 (mod 7), x ≡ 3 (mod 11) and x ≡ 16 (mod 19): $x \equiv a^1b_1\frac{M}{p} + a_2b_2\frac{M}{q} + a_3b_3\frac{M}{r}$ (mod n) x ≡ [(6)(6)(11.19) + (3)(1)(7.19) + (16)(1)(7.11)] (mod 1463) x ≡ 9155 (mod 1463)→ x = 377
- x ≡ 1 (mod 7), x ≡ 8 (mod 11) and x ≡ 16 (mod 19): $x \equiv a^1b_1\frac{M}{p} + a_2b_2\frac{M}{q} + a_3b_3\frac{M}{r}$ (mod n) x ≡ [(1)(6)(11.19) + (8)(1)(7.19) + (16)(1)(7.11)] (mod 1463) x ≡ 3550 (mod 1463)→ x = 624
- x ≡ 1 (mod 7), x ≡ 3 (mod 11) and x ≡ 3 (mod 19): $x \equiv a^1b_1\frac{M}{p} + a_2b_2\frac{M}{q} + a_3b_3\frac{M}{r}$ (mod n) x ≡ [(1)(6)(11.19) + (3)(1)(7.19) + (3)(1)(7.11)] (mod 1463) x ≡ 1884 (mod 1463)→ x = 421

Now, we can take the advantage of symmetry to get the other results:

$$x = 1463 - 1422 = 41$$
$$x = 1463 - 377 = 1086$$
$$x = 1463 - 624 = 839$$
$$x = 463 - 421 = 1042$$

Finally, the original message must be one of 1422, 377, 624, 421, 41, 1086, 839 and 1042.

8. COMPARISON WITH RSA AND RABIN CRYPTOSYSTEM

The cryptosystems RSA, Rabin and H-Rabin are very similar (Diplomă, 2008). All the three of them 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 and H-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 (Arpit and Mathur, 2013; Haraty *et al*., 2006). Which makes the Rabin cryptosystem and H-Rabin cryptosystems are more secure in this way than the RSA. However the H-Rabin cryptosystem is more secure than Rabin cryptosystem since in H-Rabin cryptosystem there exist eight square roots of c mod n ($c = m^2$ mod n) in the encryption process, so there are eight possible messages m. But in H-Rabin cryptosystem, there are only six possible messages. That would make the security of H-Rabin cryptosystem is better than Rabin cryptosystem since the decryption process would be more complicated than Rabin cryptosystem.

On the other hand, the Rabin and H-Rabin encryption processes are more efficient than RSA's, because the Rabin and H-Rabin encryption processes require to compute roots modulo n and that's more

efficient than the RSA which requires the computation of nth powers. About the decryption process both apply the Chinese remainder theorem (Arpit and Mathur, 2013). The disadvantage in decryption process of Rabin cryptosystem or H-Rabin cryptosystem is that in Rabin cryptosystem, the process produces four results, three of them false results. But, the process of H-Rabin cryptosystem produces eight results, seven of them false results, while the RSA cryptosystem just gets the correct one.

9. DISCUSSION

The Rabin cryptosystem, published in January 1979 by Michael O. Rabin (Arpit and Mathur, 2013), is an asymmetric cryptosystem where the private key is composed of two primes, p and q and a public key composed of n = p.q. Its security is based on the hardness of factoring n. Since the integer factorization is one of the open conjectures in mathematics. In this study, I suggest a modification for the Rabin cryptosystem, called H-Rabin cryptosystem, by increasing the number of its private keys to three keys that are the prime numbers p, q and r in the public key n = p.q.r. However its security is also based on the hardness of factoring n, it gives a better defense against some attacks more than the Rabin cryptosystem. Because finding three private keys using the prime factorization is much more harder than figuring two keys.

10. CONCLUSION

This H-Rabin cryptosystem is a public key cryptosystem where the private key is composed of three primes, p, q and r and a public key composed of n = p.q.r. It is based on the hardness of factoring. It is not hard to compute a square roots modulo composite if the factorization is known, but very complex when the factorization is unknown. In terms of computational performance, Rabin encryption is extremely fast 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, eight possible results will be obtained after applying the Chinese Remainder Theorem to solve the systems of congruence's. The H-Rabin cryptosystem has three private keys that are p, q and r, while the Rabin cryptosystem has two private keys p and q. Therefore, figuring three private keys using the prime factorization is much more harder than figuring two keys. This study gives a general idea about H- Rabin cryptosystem and its encryption and decryption procedures are shown with help of Chinese Remainder Theorem along with suitable example. Therefore, this study suggests a modification of Rabin Cryptosystem, called H-Rabin cryptosystem, that can make the Rabin cryptosystem more immune against some attacks than before. That leads to an increase of the confidence in the security of using the H-Rabin cryptosystem in any application using the Rabin Cryptosystem.

11. REFERENCES

Arpit, K.S. and A. Mathur, 2013. The rabin cryptosystem and analysis in measure of chinese reminder theorem. Int. J. Sci. Res. Public., 3: 1-4.

Diplomă, L., 2008. Public-key cryptography: The rsa and the rabin cryptosystems. Universitatea"babeş-bolyai"cluj-napocafacultatea de matematică şi informatică departamentul informatică.

Haraty, R.A., A.N. El-Kassar and B. Shibaro, 2006. A comparative study of rsa based digital signature algorithms. J. Math. Stat., 2: 354-359. DOI: 10.3844/jmssp.2006.354.359

Jeffrey, H., P. Jill and H. Joseph, 2008. An Introduction to Mathematical Cryptography. 1st Edn., Springer, Berlin, ISBN-10: 0387779949, pp: 540.

Rabin, N.S., 2014. The rabin cryptosystem. University of paderborn.

Rosen, K.H., 2005. Elementary Number Theory and Its Applications. 5th Edn., United State of America, Boston, ISBN-10: 0201870738, pp: 290.

Schmidt-Samoa, K., 2006. A new rabin-type trapdoor permutation equivalent to factoring. Electr. Notes Theoret. Comput. Sci., 157: 79-94.

Sorin, I., 2007. General secret sharing based on the chinese remainder theorem with applications in e-voting. Electron. Notes Theoret. Comput. Sci., 186: 67-84. DOI: 10.1016/j.entcs.2007.01.065

WFE, 2014. Rabin cryptosystem. Wikipedia, The Free Encyclopedia.