Modified Rabin Cryptosystem

Vishnu Priy Agnihotri[1]

Abstract— **In this paper, a Deterministic Rabin Cryptosystem algorithm is proposed. The algorithm works without use of complicated mathematical objects such as Jacobi symbol and the Dedekind's sums theorem.It is based on Padding mechanism which is used to distinguish the original plaintext from other outputs obtained through decryption.**

Keywords–Rabin Cryptosystem, Encryption, Integer Factorization,Padding

I. INTRODUCTION

Crptography or cryptology is the study and practice of various techniques used to secure communication between two relevant parties. It is primarily concerned with Confidentiality(information not being understood by third party), Integrity(Information cannot be altered), non-repudiation(sender should be clear in his intentions) and Authentication(Sender and receiver can confirm each other). Nowadays cryptography is being used almost every where to secure data and communication[3]. Three types of Cryptographic techniques are:

1) Symmetric Key Cryptography:: Where the sender and the reciever have the same key.Sender uses the key to encrypt plain text and the receiver uses the same key to decrypt the received encrypted text.
2) Hash Function::No key is used in this algorithm. Just a fixed-length hash value is computed as per the plaintext.
3) Public-Key Cryptography::also known as asymmetric-key cryptography, is a process that uses a pair of related keys – one public key and one private key – to encrypt and decrypt a message and protect it from unauthorized access or use.

The Rabin Cryptosystem is a public-key cryptographic algorithm invented by Michael Rabin[2]. It has very low computational cost compared to the well known RSA cryptosystem and it has been proven to be as difficult as the integer factorization problem[1]. Disadvantage of this cryptosystem is that decryption produces four possible answers out of which only one is the original plaintext.

II. EXISTING WORK

The section below describes in detail the various steps in Rabin cryptosystem algorithm and briefly describes various methods used by researchers to recover the original plaintext from four decrypted outputs.

A. Key Generation

1) Two prime numbers p and q are chosen such that p is not equal to q and both are congruent to 3(mod4).These p and q are the private keys which the receiver will use to decrypt the message later on.
2) Multiply p and q . Let's call this product n. This n is the public key which the sender uses to encrypt the message.
3) Publish n as public key and save p and q as private key.

B. Encryption

1) The sender receives the public key n.
2) The message to be sent is converted to number. Let this number be m.
3) Encryption is done with the formula: $C=m^2 \bmod n$
4) Send C to the receiver.

C. Decryption

1) Accept C from the sender.
2) Calculate integers a and b using Extended Euclidean GCD such that, a.p+b.q=1

[1] Vishnu Priy Agnihotri, BT18CSE018, Department of Computer Science and Engineering,NIT Uttarakhand

3) Compute r and s using formula:
   r=C$^{(p+1)/4}$ mod p
   s=C$^{(q+1)/4}$ mod q
4) Calculate X and Y using following formula:
   X= (a.p.r + b.q.s) mod p
   Y= (a.p.r - b.q.s) mod q
5) Four possible plaintexts are X, n-X ,Y, n-Y

One of these four values is the original plaintext m, although which of the four is the correct one cannot be determined without additional information.

D. *Example*

Let the two private keys p and q be 7 and 11 respectively.Therefore n is 77.
Take the plaintext number m to be 20.
Ciphertext (C) thus becomes C=m^2 mod n = 400 mod 77 = 15.
Decryption takes place now.
Compute r=C$^{(p+1)/4}$mod p =15^2 mod 7=1
Compute s=C$^{(q+1)/4}$mod q= 15^3 mod 11=9
Using the extended euclidean algorithm: a=-3 and b=2.
X=(-3.7.9-2.11.1)mod77 =64
Y=(-3.7.90-2.11.1)mod 77=20
Other two roots are 77-64=13 and 77-20=57.
These four are the decrypted results out of which we can see Y=20 is the original plaintext.

III. Proposed Modification

As in the previous example we saw that the four-to-one decryption setting of the rabin cryptosystem leads to a decryption failure as no indicator for selecting the correct plain text is given. In this section modification to the rabin cryptosystem is proposed so as to make it deterministic by using padding mechanism. A redundant info regarding the original plaintext is combined with it and out of the four generated roots whichever satisfies our criteria is the original plaintext.Following are the steps in the modified algorithm.

A. *Key Generation*

With respect to the original rabin cryptosystem key generation remains the same.

B. *Encryption*

After receiving the public key n and the plaintext m, the sender has to perform some preprocessing on the plaintext.This preprocessing involoves concatenating three digits to the end of the plaintext before applying encryption formula to it.

1) If the number m is even we concatenate 1 to the end of it else 0.Let this new number be e.
2) If the binary representation of m has even number of set bits i.e. number of 1's we concatenate 1 to the end of e else 0.Let this number be f.
3) If the number of digits in m is even we concatenate 1 to the end of f else 0.Let this number be g.
4) We now encrypt g using the formula C=g^2 mod n

Taking one example. Let m be 3727.

1) Since 3727 is odd, we concatenate 0 to it. Therefore e=37270
2) Binary representation of 3727 is 111010001111 , which has even number of set bits. f=372701
3) 3727 has even number of digits. g= 3727011. This g will be encrypted.

C. *Decryption*

Decryption is performed same as the original cryptosystem.

After we receive our four roots from the decryption, check is performed on each of the roots and whichever satisfies our criteria is the original plaintext. Our criteria check will confirm that there was a plaintext on which above mentioned preprocessing was done and then was sent to the encrypter.We check each root one by one.Let the root in consideration be r.

1) Last three digits of r should either be 0 or 1.
2) If r/1000 is even then third last digit of r must be 1 else if it is odd then it should be 0.
3) If r/1000 has even number of set bits in binary representation then r's second last digit must be 1 else if it has odd number of set bits then it should have 0.
4) If r/1000 has even number of digits then r should have 1 as last digit else 0.

Taking our example from previous section. Plaintext m=3727 , after pre-processing we passed g=3727011 into the encrypter.

From decryption we will receive four roots:58888500,13000,62602533,3727011. Let's call them a,b,c and d respectively.

a:Since third last digit of a is 5, it has failed our check and we can be sure that it is not our original plaintext.

b:It has last three digits 0 so it is valid.

Next b/1000 is odd so it must have 0 as third last digit which is true.

b/1000 has binary representation 1101 which has odd number of set bits so it must have 0 as its second last digit which is true.

b/1000 has even number of digits so it must have 1 which is not the case. Therefore b is not our answer.

c:Last three digits of c are not 1's and 0's hence it is invalid.

d: Last three digits of d are 1's and 0's hence it is valid.d/1000 is odd and has 0 as third last digit which is true. d/1000 has even number of set bits so it should have 1 as second last digit which is true.

d/1000 has even number of digits so its last digit should be 1 which is true.Hence d is our answer and the original plaintext is d/1000.

IV. Experimental Analysis

Implementaion of this algorithm can be found here[12]. This modified rabin cryptosystem was tested with various combinations of private keys and plaintexts. Decryption failure wherein the algorithm failed to determine the original plaintext was less than 3%. The code for this test can be found here[11].This algorithm performed slower than the original one as it was more complicated both time and space wise.

V. Limitations and Future Scope

This proposed method has a few weaknesses. Most notably it has an increased complexity with respect to the original one as more calculations are being performed per encryption and decryption to figure out the original plaintext.It is more resource heavy. With respect to the original cryptosystem , it has a lower plaintext space as three digits are being concatenated to the end of the plaintext. In future more digits can be concatenated to the end of the plaintext to make it more secure against decryption failure. As an example we can concatenate 1 to the end of it if the sum of its digits is even else 0. Further research can be done in this direction to improve the current algorithm.

VI. Conclusion

The proposed modification is one of various methods that can be employed to determine the original plaintext.This modified algorithm was able to determine the original plaintext in most cases with the help of padding.In future work, there is a scope in improving the proposed technique so that it is applicable for all messages.

References

[1] Roman Novak. SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation. In Public Key Cryptography, pages 252–262. Springer,2002

[2] M. Rabin, Digitalized signature as intractable as factorization,Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1978.

[3] B. Schneier, Applied cryptography, Wiley, 1996.

[4] J.A. Buchmann, Introduction to Cryptography, Springer, New York,1999.

[5] J. Hoffstein, J. Pipher, J.H. Silverman, An introduction to mathematical cryptography, Springer, New York, 2008.

[6] A.J. Menezes, P.C.V. Oorschot, and S.A. Vanstone. Handbook Of Applied Cryptography. CRC Press, 1997.

[7] Steven D Galbraith. Mathematics Of Public Key Cryptography. Cambridge University Press, 2012.

[8] M.A. Asbullah, M.R.K. Ariffin,Rabin-p Cryptosystem: Practical and Efficient Method for Rabin based Encryption Scheme arXiv:1411.4398v1[cs.CR] 17 Nov 2014,1-13

[9] H-RABIN CRYPTOSYSTEM ,Hayder Raheem Hashim,Journal of Mathematics and Statistics 10 (3):304-308, 2014,ISSN: 1549-3644

[10] Bhatt, Manish and Suman, Shweta and Deshmukh, Maroti, (DRC): Deterministic Rabin Cryptosystem (April 27, 2018). Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India) on March 26-27, 2018, Available at SSRN: https://ssrn.com/abstract=3170174 or http://dx.doi.org/10.2139/ssrn.3170174

[11] https://github.com/iamvpa/DeterministicRabinCryptosystem/blob/main/drcFailTest.cpp

[12] https://github.com/iamvpa/DeterministicRabinCryptosystem/blob/main/DRabinCryptosystem.cpp

[13] https://www.math.auckland.ac.nz/ sgal018/crypto-book/ch24.pdf

[14] https://www.geeksforgeeks.org/rabin-cryptosystem-with-implementation/

[15] https://en.wikipedia.org/wiki/Rabin_cryptosystem