New Proposed Methods to Factorize the Modules of Rabin's Cryptosystem

Sattar B. Sadkhan and Haythem Ahmed

Abstract

This paper provides a new method to factorize the Module value of The Rabin's Cryptosystem. One of the method based on finding the value of p from the a specified table used in Rabin crypto-system.. The second method aims to factorize n (where n= p-q) by using a new algorithm on the definition of the generator.

Keywords: Public key cryptosystem, Rabin cryptosystem, attack, cryptanalysis, Cryptography, Factorization method.

1. Introduction

Cryptography is one of the mathematical applications that is useful in transmitting the data through an insecure communication channels, which is considered as a worst case. It is also used in the international banks communication and military communications. There are some mathematical concepts which are considered as a major important aspects in this field, prime number generation , primality testing, solution of system of congruence, and factorization of polynomials over finite fields.

Iin 1976, Diffie and Hellman published a paper about the public- key cryptosystem [1]. They proposed to build a cryptosystem that doesn't require a secure channel, but nevertheless offers the possibility for secret communication. Diffie and Hellman proposed such system for distributing the secret key to be used in conventional cryptosystem over the insecure communication channel.[2]. This is a revolutionary type of cipher system which could overcome many of the key management problems have plagued cipher systems since the first day of their conception. RSA type is a branch of public key crypto system, RSA named after the three inventors, RSA gets its security from the difficulty of factoring large numbers, the public and private key are functions of (100 digits or even larger) prime numbers . The difficulty of factoring large integers has a vital parameter in estimating the security achievable in many secure data schemes and conversely factoring techniques are potentially a tool for cryptanalyst. In 1979, Rabin proposed his system which is based on factoring large number, and the result of decipherment algorithm is four plaintext messages, one of them is the correct one. In 1980, William modified the Rabin's cryptosystem under the some conditions for choosing the prime numbers [3]. In 1983, Kothari proposed a hybrid cryptosystem depending on RSA and Rabin's cryptosystem [4]. In 1989, Shimada modified Rabin's Cryptosystem by the extension Rabin's encryption function under some conditions on the secret keys by using Jacobean's symbol [5]. In 1995, Abdul Sattar S. studied some public key crypto systems depending on some evaluation parameters and proposed primality testing methods using Legender's Symbol. He also proposed an analysis study to decrease deciphering time by determining the random numbers which are used to factor the polynomials in deciphering algorithms [6]. Haythem in 1999, Provided a new supporting mathematical tools for primality testing to enhance the attacking efforts aimed towards these cryptosystems [7].

This paper provides a new method to factorize the Module value of The Rabin's Cryptosystem. One of the method based on finding the value of p from the a specified table used in Rabin crypto-system.. The second method aims to factorize n (where n= p-q) by using a new algorithm on the definition of the generator.

2. Rabin's Public Key Cryptosystem

Michael Rabin discovered what is called a version of RSA, although it is more properly regarded as a public key cryptosystem in it's own right. During its early history, this system was considered of theoretical, but not practical interest because of a " fatal flaw " that made it vulnerable to chosen plaintext attack. However, there is a way around the flaw, making this system a real competitor to RSA [8]. Rabin's Cryptosystem is a good alternative to the RSA cryptosystem, though both depends on the difficulty of factoring for their security.

Rabin's proposed his system in 1979, which gets it's security from the difficulty of finding square roots modulo a composite number [9].

Key generation method

Each user choose two primes p and q, both congruent to 3 mod 4, and forms the product n = p*q .
Hence: The public key is (n) , and the secret (private) key is (p and q) .

Encryption

To encrypt the message M, where: M= { m | 0< m ≤ n-1 }, the cipher text has the form $E(M) = C \equiv m^2 \bmod n$.

Decryption

Given the cipher text C, use the formulas below to calculate the four square roots modulo n of C : M_1, M_2, M_3, and M_4. One of the four is the original message M, a second square root is n-m, and the other two roots are negatives of one another, but otherwise random looking. Somehow one needs to determine the original message from the other three roots. In the special case in which both primes when divided by 4 give remainder 3, there are simple formulas for the four roots:
Formulas for the four square roots of a square C. Compute:
$M_1 = c^{(p+1)/4} \bmod p$
$M_2 = (p-c^{(p+1)/4} \bmod p$
$M_3 = (q-c^{(q+1)/4} \bmod p$
$M_4 = (q-c^{(q+1)/4} \bmod p$
Now compute the integers a & b :
$a = q(q \bmod p)^{-1} \in z_p$
$b = p(p \bmod q)^{-1} \in z_q$
the four possible solutions are :
$M_1 = (am_1 + bm_3) \bmod n$
$M_2 = (am_1 + bm_4) \bmod n$
$M_3 = (am_2 + bm_3) \bmod n$
$M_4 = (am_2 + bm_4) \bmod n$
In case M and hence C have p or q as a divisor, the formulas will only yield two square roots, each also with p or q as a factor. For the large primes used in instance of Rabin, there is a vanishing small chance of this happening.

However Rabin's cryptosystem has the drawback that it's encryption transformation is not one – to – one for all messages, there are 4 to 1 ambiguity in the decrypted messages [6].

Example -1:

Let p=7 and q=11, to encrypt the set M = { m | 0< m ≤ 38 }, the result will be :

M = { 1 2 3 4 5 6 7 8 9 1
0 11 12 13 14 15 16 17 18 19 20
21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 }.
Then the cipher messages will be :
C = { 1 4 9 16 25 36 49 64 4 23
44 67 15 42 71 25 58 16 53 15
56 22 67 37 9 60 36 14 71 53
37 23 11 1 70 64 60 58 }.

To decrypt this cipher codes , the table-1 represents the resulted (M_1, M_2, M_3, M_4) for each cipher text resulted in the enciphering process .

3- Attacking Methods on Rabin Crypto-system

3-1 The first Lipton's Method

Lipton assumed that two plain texts M_1 and M_2 are encrypted modulo n and the difference between M_1 and M_2 is a constant t , so M_1 and M_2 can be obtained as follows [4] :
$C_1 = M_1^2 \bmod n$
$C_2 = M_2^2 \bmod n$
$= (M_1 + t)^2 \bmod n$

then $M_1 = \{ (C_2 - C_1 - t^2) / 2t \} \bmod n$

$M_2 = M_1 + t$

Example -2:

Let t= 19 , $C_1 = 2403$, $C_2 = 1452$ and n = 3337, find M_1 and M_2.

hence :

$M_1 = \{(1452 - 2043 - 361) / 2*19 \} \bmod 3337 = 668$

And $M_2 = 687$

3-1 The second Lipton's method

Lipton assumed that M is encrypted in two different modulo (n_1 , n_2) , then the analyst could know M as follows [4] :

a- Find : x ,y such that :

$x = (y*n_2 + C_2 - C_1) / n_1$, choosing a random value to y such that x be an integer .

b- Compute the value of t where

$t = \lfloor -x / n_2 \rfloor$

Now $M = (C_1 + (x + t*n_2) n_1)^{1/2}$

Example -3 :

If we have m = 54 and $n_1 = 65$, $n_2 = 77$, $C_1 = 67$. To find M by using the second **Lipton method** :

Let y = 37 then x = 44 & t = 0 , hence M = 54

4- New results for Rabin's Cryptosystem

The main efforts have been concentrated towards the cryptanalytic attack on the Rabin's Cryptosystem . The well known methods for attacking Rabin's system are iteration method and Fermat's factorization method .

4-1 The First New Attack Method

To cryptanalysis the **Rabin's Cipher text** , let x be the first integer grater than 1 satisfying the congruencies $x^2 \equiv 1 \bmod n$, then each of (x) and it's complement (n-x) are called a generator of n . This method based on finding a generator x in the ring Z_n , by using any algorithm, and then built a table by the following algorithm :

Step 0 : generator = x

Step 1 : I=1

Step 2 : Let $M_1 = 1$, $M_2 = x$, $M_3 = n-1$, $M_4 = n-x$

Step 3 : I = I + 1

Step 4 : Let $M_1 = 1$, $M_2 = (M_{2i-1} + x) \bmod n$, $M_3 = n-1$, $M_4 = n-M_2$

Step 5 : I < (n-1) / 2 Go step 3 else stop

Example -4:

To find all the plain text in Z_{77} . Following the described algorithm the result is shown in table (2) in appendix.

Not that

- This table is provided for n/2 because the second half of the table is symmetric.
- This method for small n is efficient .

4-2 The Second New Attack Method :

proposition

Given a cipher C, then we should find the first integer k such thst : $k^2 \bmod n = c$ then m= k or n-k or kx (mod n) or n-k (mod n) .

The first method

If n = p*q where p<q , then the distance between first similar two ciphering codes represent the prime p .

The second method

If n = p*q where p<q , then p is the first integer k satisfying the equation k = kx (mod n) where x is the generator of n .

Note :

For first method and second method see table (2) .

5- Conclusion

In Rabin's Cryptosystem

a- The definition of the generator is a great contribution in attack direction because this definition opened many attacking ways on Rabin's cryptosystem. The first method is to build a table by a new algorithm depending on the definition to find all the possible plain text (M_1, M_2 , M_3 , M_4) this method not

efficient with large number because the table will be too long .

b- In the second attack, during the table preparation we can stop just the cipher text C_j appear which is similar to any C_j (i<j) and the distance between C_i and C_j represent the prime number p .

References:

[1] Henery Beker and fred Piper, " Cipher system ", ISBN publisher, 1982.

[2] Bruce S. ," Applied Cryptography ", second edition , John Wiley and Sons, Inc. 1986.

[3] H.c. WILLIAM, " a Modification of RSA Public Key Encryption procedure ", IEEE transaction on Information Theory, IT-26, 1980.

[4] lauy A. Alhani," Mathematical Analysis for Crypto Methods of Public Key Cryptosystems and Proposing a New Cipher systems ", Ph.d. thesis, AL-Mustansirayah University, Mathematical Science DEPT. , Baghdad, Iraq, 1998.

[5] M. shimada, " another Practical Public Key cryptosystem ", Electronic Letters, 5th November 1992, Vol. 28, No. 23.

[6] Abdul Sattar S. Alshamari, " Analytical Study of some Public key cryptosystems depending on some evaluation parameters", M.Sc. Thesis, University of Technology, Applied Mathematics Dept. Baghdad, Iraq, 1995.

[7] Haythem G. Ahmed, " Mathematical analysis of RSA and Rabin Cryptosystems", M.Sc. Thersis, AL-Mustansiryia University, Mathematical Dept., Baghdad, Iraq, 1999.

[8] Neal F. Wanger," The Laws of Cryptography : Rabin's Version of RSA ", 2002.

[9] M. O. Rabin , " Digitalized signature and Public Key Functions as intractable as factorization ", technical Report, MIT/ LCS/ Tr, MIT Lab. Computer Science , Cambridge, Jan. 1979.

Appendix

Table (1)

C1	M1	M2	M3	M4
1	1	43	34	76
4	9	2	75	68
9	25	74	3	52
16	4	18	59	73
25	16	72	5	61
36	71	50	27	6
49	70	7	70	7
64	36	8	69	41
23	67	32	45	10
44	11	11	66	66
67	23	65	12	54
15	64	57	20	13
42	14	63	14	63
71	15	29	48	62
25	16	72	5	61
58	60	39	38	17
16	4	18	59	73
53	58	30	47	19
15	64	57	20	13
56	56	21	56	21
22	22	22	55	55
67	23	65	12	54
37	53	46	31	24

Table (2)

C1	M1	M2	M3	M4

1	1	34	76	43
4	2	68	75	9
9	3	25	74	52
16	4	59	73	18
25	5	16	72	61
36	6	50	71	27
49	7	7	70	70
64	8	41	69	36
4	9	75	68	2
23	10	32	67	45
44	11	66	66	11
67	12	23	65	54
15	13	57	64	20
42	14	14	63	63
71	15	48	62	29
25	16	5	61	72
58	17	39	60	38
16	18	73	59	4
53	19	30	58	47
15	20	64	57	13
56	21	21	56	56
22	22	55	55	22
67	23	12	54	65
37	24	46	53	31
9	25	3	52	74
60	26	37	51	40
36	27	71	50	6
14	28	28	49	49
71	29	62	48	15
53	30	19	47	58
37	31	53	46	24
23	32	10	45	67

11	33	44	44	33
1	34	1	43	76
70	35	35	42	42
64	36	69	41	8
60	37	26	40	51
58	38	60	39	17