A mathematical model for ascertaining same ciphertext generated from distinct plaintext in Michael O. Rabin Cryptosystem

Md. Shamim Hossain Biswas

Abstract— Michael O. Rabin Cryptosystem can generate same ciphertext form different plaintext as well as multiple plaintext from single cyphertext. There are a number of techniues to reveal original plaintext. But none of them can seperate same cyphertext against each plaintext generated from modular reduction arithmetic. If question arises about how one can distinguish particular ciphertext against each plaintext, to answer those questions, I design a new mathematical model for identifying same ciphertext against each plaintext and it also facilitates message encryption and decryption. The proposed mathematical model constructiond based on quadratic root of quadratic residue, quadratic quotient, floor function and absolute value counting in order to identify the ciphertext against the plaintext. In particular. When same number of residues generated from multiple plaintext applying modular reduction arithmetic. The proposed crypto intensive technique uses symmetric key using Diffie-Hellman key exchange protocol. The advantage of proposed crypto intensive technique is intended receiver getting only one plainvalue distinguishing the ciphertext against the plaintext. The proposed crypto teachnique requires less time complexity and probabily secure against man-in-the-middle, chosen plaintext and cyphertext attack.

Index Terms—Michael O. Rabin's Encryption and signature schem,e, Diffie-Hellman key exchange protocol, modular arithmetic, Bezout's Coefficient, Extended Euclidean Algorithm, Chinese Remainder Theorem, Polynomials, Legendre Symbol, Congruence, ASCII- Code, Floor and Absolute Value function.

1 Introduction

Since[1-2] publication on January (1976, 1979) by Michael O. Rabin, a huge number of surveys had been carried out over Rabin's Cryptosystem to find out its efficiency and devise a new method for real life application. It was the first asymmetric cryptosystem in the field of public key Cryptography. Security of Rabin's encryption mechanism relies on prime integer factorization. It was not widely used due to having some computational error, but its theoretical significance widespread. The encryption mechanism used quadratic residue to produce cipher text and Decryption was accomplished by Computing two square root, Bezout's Coefficient using extended Euclidean algorithm and combining them with Chinese Remainder theorem. Similarly to the RSA and ElGamal cryptosystems, Michael O. Rabin cryptosystem is described in a ring under addition and multiplication modulo composite integer. One of the main disadvantage is to generate four results during decryption and extra effort needed to sourt out the right one out of four possibilities. In this paper I design a new crypto intensive technique based on Diffie –Hellman key exchange protocol [3], concept of square modular arithmetic from Michael O. Rabin Cryptosystem, Floor function and absolute value function. The symmetric key generates from Diffie-Hellman key exchange protocol.
The sender Bob sends a pair of integer to Alice as an encrypted text (C) = ($\lfloor m^2/K \rfloor$, $m^2 \bmod K$). After receiving, Alice decrypts the message (D) = $|\sqrt{Q.K+R}|$ and gets only one desired plain text unlike Rabin's Cryptosystem in which she gets four different decryption results. The rest of the paper is organized as a follows. Section 1.1 summarizes Overview of Michael O. Rabin cryptosystem. Ssection 1.2 gives an overview of Rabin's Signature Scheme, Section 1.3 provides an overview of Diffie-Hellman Key Exchange protocol. Section 2 gives Literature Review, Section 3.for proposed mathetical model, Section 3.1 for prposed Algorithm, Section 3.2 gives summary of proposed mathmetical model, In section 3.3 shows comparisons, Finally, Section 4, 5 give conclusion and acknowledgement.

1.1 Overview of Rabin's Cryptosystem [4]

SUMMARY:
Each entity creates a public key and a corresponding private key. Each entity A should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute n = p q.
3. A's public key is n; A's private key is (p, q).

Algorithm for Rabin's public-key encryption

SUMMARY:
B encrypts a message m for A, which decrypts.
1. Encryption. B should do the following:
   (a) Obtain A's authentic public key n.
   (b) Represent the message as an integer m {0, 1... n- 1}.
   (c) Compute c = m^2 mod n.
   (d) Send the cipher text c to A.

Algorithm for Rabin public-key Decryption
SUMMARY:

To recover plaintext m from c, A should find the four square roots m_1, m_2, m_3, and m_4 of c modulo n. The message sent was either m_1, m_2, m_3, or m_4. A decides which of these is m by ascertain replicating bits.

1. Use the extended Euclidean algorithm to find integers Y_p and Y_q satisfying $p.Y_p + q.Y_q = 1$.
2. Compute $M_p = c^{(p+1)/4} \bmod p$.
3. Compute $M_q = c^{(q+1)/4} \bmod q$.
4. Compute $x = (Y_p.p.\ M_q + Y_q.q.\ M_p) \bmod n$.
5. Compute $y = (Y_p.p.\ M_q - Y_q.q.\ M_p) \bmod n$.
6. The four square roots are x, −- x, y and−- y mod n.

For example, Key generation: Entity A chooses the primes p = 277, q = 331, and computes n = p.q = 91687. A's public key is n = 91687, while A's private key is (p = 277, q= 331).

Encryption:

Suppose that the last six bits of original messages are required to be replicated prior to encryption. In order to encrypt the 10-bit message m = 1001111001, B replicates the last six bits of m to obtain the 16-bit message m = 1001111001111001, which in decimal notation is m = 40569. B then computes $c = m^2 \bmod n = 40569^2 \bmod 91687 = 62111$ and sends this to A.

Decryption:

To decrypt c, A uses aforesaid algorithm and her knowledge of the factors of n to compute the four square roots of c mod n: $m_1 = 69654$, $m_2 = 22033$, $m_3 = 40569$, $m_4 = 51118$, which in binary are $m_1 = 10001000000010110$, $m_2 = 101011000010001$, $m_3 = 1001111001111001$, $m_4 = 1100011110101110$. Since only m_3 has the required redundancy, A decrypts c to m_3 and recovers the original message (m) = 100111100

1.2 Overview of Rabin's Signature Scheme

Rabin's Cryptosystem is composed of Key Setup, Encryption and Decryption. Key Generation step-1: Let, Alice chooses two random prime numbers P and Q. Compute public key N= P*Q she also picks a random integer ($0 \leq b < N$; publicize (N, b) as her public key material, and keep (P and Q) as her private key .

Encryption step-2:
The sender Bob creates cipher text $C=m\ (m+b) \bmod N$. *Here* uses of b is Security purpose only $(0 \leq b < N)$.

Decryption step-3:
Alice solves the quadratic equation $m^2 - m\,b + c \equiv\equiv 0 \pmod N$ to decrypt the ciphertext. Decryption involves computing square roots modulo N. Decryption consisting of $m^2 \equiv a$ (mod n). This is performed by solving $M_p = m^2 \equiv a \pmod p$ and $M_q = m^2 \equiv a \pmod q$. Pick a random integer b in range $0\ldots p$ and compute the Legendre symbol $(b^2 - 4a)$ / p i.e., $(b^2 - 4a)^{(P-1)/2}$ mod p with result p - 1 replaced by -1, until that's -1.Now setup the second degree polynomial arithmetic f and then compute the polynomial $x^{(p+1)/2} \bmod f$ and $x^{(q+1)/2} \bmod f$ using polynomial arithmetic modulo the polynomial f. Compute Bezout's coefficient using extended Euclidean algorithm and combine these using the Chinese Remainder Theorem yielding four solutions in most cases, and picking the right one in some way.

Example:

Step 1. Let, two random prime number p= 41, q= 53 and public key: N= p. q =1273 Message m=92. Cipher text $c = m^2 \bmod N = 1945$. Now compute $M_p = m^2 \equiv a \pmod p = 18$ and $M_q = m^2 \equiv a \pmod q = 37$.

Step 2. Choose a random b = 2 satisfying the condition and setup a polynomial $f = x^2 - b.\ x + M_p$ *with* coefficients in Z_{41}, that is $f = x^2 + 39x + 18$ similarly b = 4 satisfying the condition and setup a polynomial $f = x^2 + 49x + 37$ with coefficients in $Z_{53;}$ x is the variable of the polynomial and has no particular value.

Step 3. Compute the polynomial $x^{(p+1)/2} \bmod f = x^{21} \bmod f$. The binary representation of the exponential order (21) is 10101, and compute x^2, x^4, x^5, x^{10}, x^{20} *and* finally $x^{21} \bmod f$ by left-to-right binary exponentiation.
Computation of $x^2 \bmod f$ that is x^2−- $(x^2 + 39x + 18)$, that is $2x+23$
Computation of $x^4 \bmod f$ that is $4x^2 + 10x + 37 - 4(x^2 + 39x + 18)$, that is $18x+6$.
Computation of $x^5 \bmod f$ that is $18x^2 + 6x$− - $(x^2 + 39x + 18)$, that is $x+4$.
Computation of $x^{10} \bmod f$ that is $(x+4)^2 \bmod f$ that is $10x+39$.
Computation of $x^{20} \bmod f$ that is $(10x+39)^2 \bmod f$ that is $37x+8$.
Computation of $x^{21} \bmod f$ that is $37x^2+8x \bmod f$. Finally, the x term has surprised leaving 31. Thus $m^2 \equiv a \pmod p$ has solution $M \in \{10, 31\} \pmod p$.

Step 4. Compute the polynomial $x^{(q+1)/2} \bmod f$ that is $x^{27} \bmod f$ using polynomial arithmetic modulo the polynomial f. The binary representation of the exponential order (27) is 11011, and compute x^2, x^3, x^6, x^{12}, x^{13}, x^{26} and finally $x^{27} \bmod f$ by left-to-right binary exponentiation. Similar computation of step 3. Solve $m^2 \equiv a \pmod q$, with solution $M \in \{14, 39\} \pmod q$.

Step 5. Compute the Bezout's Coefficient using Extended Eclidean Algorithm those are $Y_p = 22$, $Y_q = -17$

Step 6.Computation $R_1 = (Y_p.p.\ Mq_1 + Yq.\ q.\ M_{p1}) \bmod N = 728$, $R_2 = -R_1 \bmod N = 1445$, $R_3 = (Y_p.\ p.\ M_{q2} - Y_q.\ q.\ M_{p2}) \bmod N = 2081$, $R_4 = -R_3 \bmod N = 92$, Hence, the potential results are m = {728, 1445, 2081, 92} by applying Chinese remainder theorem.

ISSN 2229-5518

1.3 Diffie-Hellman Key Exchange protocol [5]

The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography [8]. It is generally referred to as Diffie-Hellman key exchange protocol. A number of commercial products employ this key exchange technique. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption and decryption of messages. The algorithm itself is limited to the exchange of secret values. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms

Global Public elements	q is a prime number which can define a domain so called curve area or elliptic curve, α is a primitive root of q such thatα α < q.
Key Generation for user A	Select private key X_a , such that $X_a < q$. Calculate public key $Y_a = \alpha^{xa} \bmod q$
Key Generation for user B	Select private key X_b such that $X_b < q$. Calculate public key $Y_b = a\alpha^{xb} \bmod q$
Secret key for user A	$K= (Y_b)^{xa} \bmod q$
Secret key for user B	$K= (Y_a)^{xb} \bmod q$

Example:

An integer number q = 353 that is domain size and its primitive root αα = 3. A and B select secret keys A = 97 and B = 233, respectively.

Each of them computes public key:
A computes $X = 3^{97}$ mod 353 = 40.
B computes $Y = 3^{233}$ mod 353 = 248.

They compute secret key in the following ways by exchanging public key between each other.

A computes $K = (Y)^{A}$ mod 353 = 24897 mod 353 =160.
B computes $K = (X)^{B}$ mod 353 = 40233 mod 353 = 160.

2. Literature Review

There are many surveys have been dedicated over Rabin's cryptosystem. Recently various modifications of Rabin's cryptosystem have been published in different scientific journals.

Hayder Raheem Hashim [6] proposed an update methodology that used three private keys instead of two. Consequently, the eight non-deterministic plaintext generates from one cypher text. One of them is real plaintext. The advantage of this technique is to make confusing attacker while it is very annoying to receiver as extra effort is required to distinguish original plaintext out of eight text.

Yahia Awad et al. [7] proposed a deterministic method depending on the domain of Gaussian Integer to select right plaintext among four decryption result. Recipient can decide particular plain text form four possible decryption result by selecting obtained square root with redundancies in its imaginary part (a + bi). This is the main benefit of using Gaussian integer technique. The disadvantage, on the other hand, same cyphertext can be generated from different plaintext due to having modular reduction arithmetic. For example, for the four plaintext (m) = {13, 20, 57, 64}, the same cipher text c=15.

Manish Bhatt et al.[8] extended a deterministic technique adding duplicating bits at the beginning of plaintext before encryption. Added replicating bits reflected within one decrypted text among four possible plaintext. The annoying thing is other three false result that refers to time complexity and memory complicity.

Masahiro Kaminaga, et al,. [9] discussed a fault attack technique on modular exponentiation during Rabin's encryption where a complicated situation arose in case of message reconstruction when message and public key were not relatively prime. They also provided a rigorous algorithm to handle message reconstruction.

Haytham Gani [10] performed study over Rabin and RSA Cryptosystem and provided insightful discussion. The computation speed of RSA and Rabin's Cryptosystem were roughly same. Both algorithm's security relied on prime integer factorization.

Preeti Chandrakar [11] discussed about a secure two factor remote authentication scheme using Rabin Cryptosystem. This paper showed an extended usages of Rabin's cryptosystem.

Xue-dong DONG, et al.[12] modified Rabin's cryptosystem using cubic residue technique which successfully removed the long cherished inconsistency so called four to one function in Rabin's cryptosystem. But, it was insecure against chosen cipher text attack that was pointed out by authors. Interestingly, the novel method of computing cubic root from a cubic residue prohibited the revealing private key.

3. Proposed Mathetical model

3.1 Prposed Algorithm

Key Generation Algorithm:

$$
\begin{aligned}
K &= (Y_b)^{xa} \bmod q \\
&= (\alpha^{xb} \bmod q)^{Xa} \bmod q \\
&= (\alpha^{xb})^{Xa} \bmod q \\
&= \alpha^{xb\,Xa} \bmod q \\
&= (\alpha^{Xa})^{xb} \bmod q \\
&= (\alpha^{xa} \bmod q)^{Xb} \bmod q \\
&= (Y_a)^{xb} \bmod q
\end{aligned}
$$

Encryption Algorithm:

$$
\begin{aligned}
Q &= \lfloor m^2 / K \rfloor \\
R &= m^2 \bmod K \\
C &= (Q, R)
\end{aligned}
$$

Decryption Algorithm:

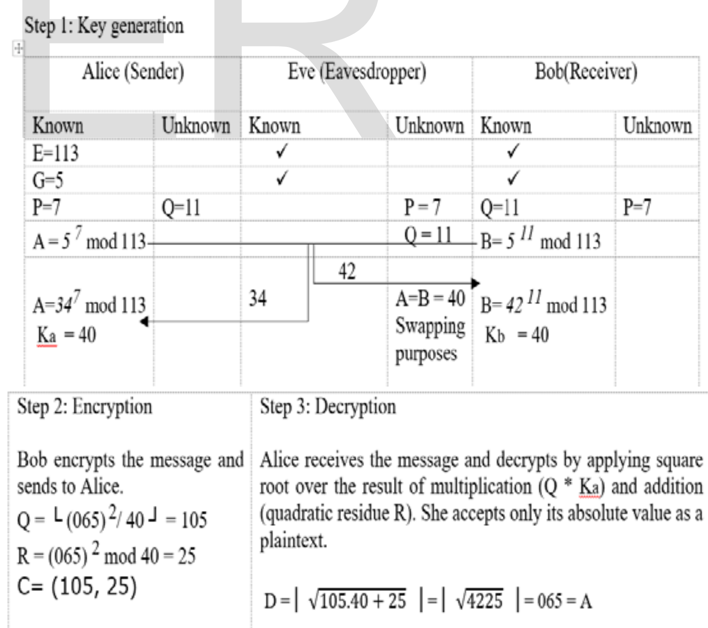
$$D = \sqrt{Q.k + R}$$

3.2 Summary of Proposed mathmetical Model

The proposed crypto technique ensures secure communication among two parties. For example, at the initial stage Alice and Bob create a shared secret key. In the second stage Bob choose a message A = 065 according to ASCII - Binary Character Table [13]. It is a character encoding standard for electronic communication. It represents text in a computer, telecommunication equipment and other devices. The following simplified snapshot of ASCII codes have been shown as an explanatory purposes of proposed crypto intensive technique. Although, total number of ASCII Codes 128.

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Then, He encrypts the message like a pair of integer using shared secret key and sends to Alice. Finally, Alice decrypt message. The following description describes entire mathematical process.



ISSN 2229-5518

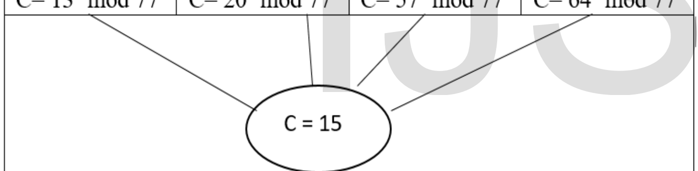
3.3 Comparisons

The comparison between proposed crypto technique and Michael O. Rabin Cryptosystem as follows.

Rabin's Crypto Scheme	Proosed Crypto technique
Cyphertext is a quadratic residue.	Ciphertext is a pair of integer
Decryption generates four plain text	Decryption generates single plaintext
It uses assymetric key	It uses symetric key
It is vulnerable against chosen ciphertext and plaintext attack.	It is not vulnerable against man in the middle attack, because, the key may be stolen but computation scheme is unknown to adversary.
Michael O. Rabin's Encription and signature scheme cannot idendify same ciphertext generated from different plaintext.	It is strong due to having ability to distinguish same Ciphertext uniquely generated from different plaintext.
Michael O. Rabin Crytposystem cannot identify same ciphertext against different plaintext.	Proposed technique can identify same ciphertext against different plain text.

A disadvantage of Michael O. Rabin cryptosystem:

$C = 13^2 \bmod 77$	$C = 20^2 \bmod 77$	$C = 57^2 \bmod 77$	$C = 64^2 \bmod 77$



The same encryption result (15) generates from four distinct plaintext M={13,20,57,64} those results cannot be identified separately by Michael O. Rabin's Cryptosystem.

An advantage of proposed crypto technique:

$R = 13^2 \bmod 77$ $Q = \lfloor 13^2 / 77 \rfloor$ C=(2,15)	$R = 20^2 \bmod 77$ $Q = \lfloor 20^2 / 77 \rfloor$ C=(5,15)	$R = 57^2 \bmod 77$ $Q = \lfloor 57^2 / 77 \rfloor$ C=(42,15)	$R = 64^2 \bmod 77$ $Q = \lfloor 64^2 / 77 \rfloor$ C=(53,15)

The proposed crypto intensive technique can uniquely identify each cipher text against plaintext.

4. Conclusion

The proposed crypto intensive mathematical technique is efficient for solving four to one mapping ciphertext. Its objective to identify each cipher text separately because modular arithmetic can generate same cyphertext from different plaintext. The proposed model can efficiently identify each cipher text separately generated form modular reduction arithmetic, while Rabin's cryptosystem fails. There is a security vulnerability in symmetric key geration stage that is man in the middle attack because it does not authenticate the participants. Even thouth proposed scheme ensures security as computation procedure is unknown to adversary.

5. Acknowledgement

I am very grateful to my family members who supported financially to conduct study because without their financial support, love and affection, this work could not be carried out. . I thank Md. Maruf Hassan for his inpiratiional advice and Dr. Md. Mostafijur Rahman (Assistant professor, Department of software Engineering, Daffodil International University) for insightful discussion during the preparation of this paper. This work is a part of academic curriculum fulfillment for MSc in software engineering.

References

[1] Michael.O. Rabin, probabilistic algorithm, algorithm and complex ity,recent results and new directions, J. F. Traub, editor, academic press, new York, 1976, pp. 21-40

[2] M.O. Rabin, Digital signatures and public key functions (1979) as Intractable as factorization, Technical report MIT-LCS-TR-212, MIT laboratory for computer science.

[3] Diffie–Hellman key exchange protocol was introduced by Malcolm John Williamson (British mathematician and cryptographer) in 1974. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[4] Michael.O. Rabin cryptosystem In: Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone.

[5] Cryptography and Network Security written by William Stallings, Fourth Edition. Page No.299. Figure 10.7. .e-text ISBN-10: 0-13-187319-9. Publisher: Prentice Hall Pub Date: November 16, 200

[6] Hayder Raheem Hashim, may 2014. H-Rabin Cryptosystem In: Journal of Mathematics and Statistics. DOI:10.3844/jmssp.2014.304.308. Researchgate publication no. 264286919

[7] Yahi Awad,, Abdul Nasser El-Kassar, Terrar Kadri. Rabin's Public-key Cryptosystem in the Domain of Gaussian Integers. In: 2018 international Conference on Computer and application (ICCA)

[8] Manish Bhatt Shweta Suman, Maroti Deshmukh*. DRC_Deterministic_Rabin_Cryptosystem. In: 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018. Researchgate publication no. 325330795

[9] Masahiro Kaminaga, Hideki Yoshikawa, Member, IEEE, Arimitsu Shikoda, Member, IEEE, and Toshinori Suzuki, Member. A Modulus Attack on Modular Squaring for Rabin Cryptosystem In: DOI 10.1109/TDSC.2016.2602352, IEEE Crashing.

[10] Haytham Gani May 2019, a Mathematical Analysis of RSA and Rab in Cryptosystem. In: ResearchGate publication no. 332834881

[11] Preeti Chandrakar, Hari Om on July 2017. An efficient two factor remote user Authentication and session key agreement scheme using Rabin Cryptosystem. In: DOI: 10.1007/s13369-017-2709-6

[12] Xue-dong DONG, Shuo Han and Yun-Feng BAI, 2017. A modifications of the Rabin Cryptosystem based on Cubic Residues. In: Communications, Information Management and Network Security (CIMNS 2017), ISBN: 978-1-60595-498-1

[13] An alphabet book for the 21st century written by Sticks and Stones.

- *Md. Shamim Hossain Biswas is currently pursuing MSc in Software Engineering at Daffodil International University in Bangladesh. https://orcid.org/0000-0002-4595-1470 PH-+8801531262445. E-mail: shamim44-165@diu.edu.bd*