IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 01-07
www.iosrjournals.org

Modified Rabin Cryptosystem through Advanced Key Distribution System

Rajdeep Chakraborty[1] , Sibendu Biswas[1], JK Mandal[2]
[1]Dept of CSE, Netaji Subhash Engineering College, Garia, Kolkata-700152, West Bengal, India,
[2]Dept of CSE, FETM, University of Kalyani, Kalyani, Nodia, West Bengal, India,

Abstract: *In this paper, an asymmetric cryptosystem Rabin Cryptosystem has been modified by adding an advanced message authentication system with it. The proposed modified Rabin Cryptosystem is a combination of symmetric and asymmetric key cryptosystem that is hybrid cryptosystem. In the symmetric part, the sender and the receiver share a secret key between themselves which is added with the plaintext to change the plaintext. The shared secret key is fixed for a session between two users. It can be different for different sessions and different users. In the asymmetric part, the modified plaintext is encrypted using Rabin Cryptosystem. Two extra values will be sent along with the cipher text to the receiver. In the decryption process, Chinese Remainder Theorem will be applied along with the two extra values which were received with the cipher text to decipher it. Then the shared secret key between the sender and the receiver will have to be applied to get the original plaintext. Even if any intruder succeeds to decipher the cipher text, he would get the modified plaintext. As he doesn't have the shared secret key, he would not be able to retrieve the original plaintext.*

***Keywords**: Asymmetric Cryptosystem, Message Authentication System, Modified Rabin Cryptosystem*

I. Introduction

Technology around us is growing very fast, and security has become the major issue in this fast growing technical world. Every moment a new threat is being produced to disrupt the security of both data and network, and to guard us against these security threats, many new security mechanisms are also being produced. Cryptography is one very ancient yet strong mechanism that saves our data from the hands of the attackers. In this paper, we have proposed a new cryptographic mechanism which is a fine combination of symmetric and asymmetric cryptosystem.

Section 1 contains the detailed description of the algorithm proposed, along with the flowchart and example of encryption and decryption process. Section 2 contains some results of the encryption and decryption procedure of the Modified Rabin Cryptosystem. It also shows the performance analysis and comparisons of the Modified Rabin Cryptosystem with RSA and Rabin Cryptosystem using several parameters. Section 3 describes the contribution of this paper in the field of cryptography. In section 4 we have drawn the conclusion of this paper. Section 5 shows the acknowledgement, and in the last section we have listed the references.

1.1 Modified Rabin Cryptosystem through Advanced Key Distribution Technique

In this paper we have modified the Rabin Cryptosystem with a secret key distribution technique that was suggested in [NEED78]. This key distribution technique is used to share the secret key between the sender and the receiver. The secret key is shared before any transaction happens between the sender and the receiver. Apart from this secret key, a public and a private key is also required. The private key is a pair of two values p and q. The public key is the multiplied value of p and q. The encryption function is (m^2 mod n) where 'm' is the message. The decryption function uses the Chinese Remainder Theorem to compute the four square roots. Then some additional values and the shared secret key are needed to retrieve the original plaintext.

1.1.1 The algorithm of the Modified Rabin Cryptosystem

Round 1: The sender A uses the receiver B's public key to encrypt a message to the receiver containing an identifier of A (ID_A) and a nonce N_1,which is used to identify this transaction uniquely. B sends a message to A encrypted with PU_A and A's nonce as well as a new nonce N_2 generated by B. A returns N_2, using B's public key. A selects secret key K_s and sends M=E (PU_b, E (PR_a, K_s)) to B. B computes D (PU_a, D (PR_b, M)) to recover the secret key [2].

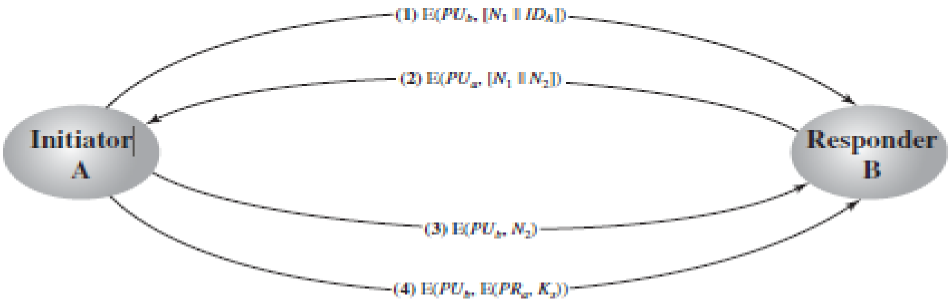

(1) E(PU_b, [N_1 || ID_A])
(2) E(PU_a, [N_1 || N_2])
Initiator A
Responder B
(3) E(PU_b, N_2)
(4) E(PU_b, E(PR_a, K_s))

Fig. 1: Secret key Distribution procedure between sender & receiver

Round 2: 'N' is the public key, which is the multiplication of p and q. p and q are the private keys, such that both p and q are congruent to 3 mod 4. A prepares the message 'M' by adding his shared secret key with the plaintext and then applying the encryption function $C=M^2$ mod N. A further calculates 2 more values a and b such that a = M mod 2 and b=1/2(1 + (M/N)).

For decryption B will have to use the Chinese Remainder Theorem to get the four square roots. At first B have to calculate M_p and M_q such that $M_p = C^{(p+1)/4}$ mod p and $M_q = C^{(q+1)/4}$mod q. Then B has to compute $+M_p$ mod p, - M_p mod p, $+M_q$ mod q and $-M_q$ mod q. These are the 4 square roots. Then take the two roots having the same parity specified by a, say x and y. Compute the numbers ½(1+(x/n)) and ½ (1+(y/n)). Then take the root corresponding to the number equal to the value of b. Thus the message M is retrieved. Now B has to subtract the shared secret key from M to retrieve the plaintext.

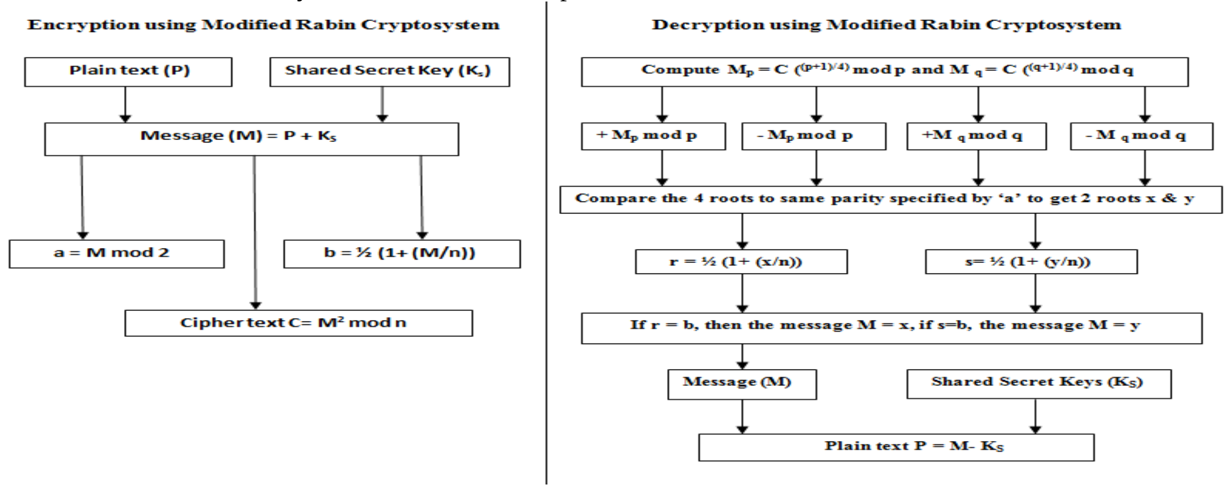

Encryption using Modified Rabin Cryptosystem
Plain text (P)
Shared Secret Key (K_s)
Message (M) = P + K_S
a = M mod 2
b = ½ (1+ (M/n))
Cipher text C= M^2 mod n
Decryption using Modified Rabin Cryptosystem
Compute $M_p = C^{((p+1)/4)}$ mod p and $M_q = C^{((q+1)/4)}$ mod q
+ M_p mod p
- M_p mod p
+M_q mod q
- M_q mod q
Compare the 4 roots to same parity specified by 'a' to get 2 roots x & y
r = ½ (1+ (x/n))
s= ½ (1+ (y/n))
If r = b, then the message M = x, if s=b, the message M = y
Message (M)
Shared Secret Keys (K_S)
Plain text P = M- K_S

Fig 2: Encryption and Decryption procedure of Modified Rabin Cryptosystem

1.1.2 Example of the Modified Rabin Cryptosystem

Sharing the Secret key

Let the I.D of 'A' is 1001 and the I.D of 'B' is 1002

A sends its I.D and a nonce N_1 = 311 encrypted with the public key of B, i.e. E (PU_B (1001||311)) to B

B sends nonce N_1 and nonce N_2 = 653 encrypted with the public key of A, i.e. E (PU_A (311||653)) to A

A sends the nonce N_2 encrypted with the public key of B i.e. E (PU_B, 653) to B

A then encrypts the secret key K_S to be shared with his own private key and then again encrypt it with the public key of B and sends X = E (PU_B, E (PR_A, K_S)) to B

B computes D (PU_A, D (PR_B, X)) to recover the secret key.

Encryption

Let A wants to send the plaintext P = 43 and the shared secret key K_S = 24

Then the message M = (P + K_S) = (43+24) = 67

Let the public key 'n' is 589

Then the cipher text C = E (67, 589) = 67^2 mod 589 = 366

a= M mod 2 = 67 mod 2 = 1

b = ½ (1+ (M/n)) = ½ (1+ (67/589)) = 0.556876

A sends the triplet (366, 1, 0.556876) to B.

Decryption

Let the private keys are: $p = 19$ and $q = 31$
B computes:
$M_p = [C^{((p+1)/4)}] \bmod p = [366^5 \bmod 19] = 9$
$M_q = [C^{((q+1)/4)}] \bmod q = [366^8 \bmod 31] = 5$
And the system of congruence $x \Xi u_i*v_i(M/m_i)$ is:
$+M_p \bmod p = 9 \bmod 19 = 9$
$-M_p \bmod p = 10 \bmod 19 = 10$
$+M_q \bmod q = 5 \bmod 31 = 5$
$-M_q \bmod q = 26 \bmod 31 = 26$
Finally we can apply the Chinese remainder theorem to compute the four square roots:
First we compute v1 and v2 such:
$n/p * v_1 \Xi 1 \bmod p \rightarrow 31 * v_1 \Xi 1 \bmod 19 \rightarrow v_1 = 8$
$n/q * v_2 \Xi 1 \bmod q \rightarrow 19 * v_2 \Xi 1 \bmod 31 \rightarrow v_2 = 18$

Now, we can compute the solutions
1) $X \Xi 9 \bmod 19$ and $x \Xi 5 \bmod 31$:
$x = (u_1 * v_1 * M/p + u_2 * v_2 * M/q) \bmod N$
$= (9*8*31 + 5*18*19) \bmod 589$
$= 3942 \bmod 589$
$= 408$
2) $X \Xi 10 \bmod 19$ and $x \Xi 5 \bmod 31$:
$x = (u_1 * v_1 * M/p + u_2 * v_2 * M/q) \bmod N$
$= (10*8*31 + 5*18*19) \bmod 589$
$= 4190 \bmod 589$
$= 67$
3) $X \Xi 9 \bmod 19$ and $x \Xi 26 \bmod 31$:
$x = (u_1 * v_1 * M/p + u_2 * v_2 * M/q) \bmod N$
$= (9*8*31 + 26*18*31) \bmod 589$
$= 11124 \bmod 589$
$= 522$
4) $X \Xi 10 \bmod 19$ and $x \Xi 26 \bmod 31$:
$x = (u_1 * v_1 * M/p + u_2 * v_2 * M/q) \bmod N$
$= (10*8*31 + 26*18*19) \bmod 589$
$= 11372 \bmod 589$
$= 181$
Finally, the original message must be 408, 67, 522 or 181.
As a=1, we take the 2 roots specified by a, as x = 67, y = 181
Now $r = ½[1+ (x/n)] = ½ [1+ (67/589)] = 0.556876$
And $s = ½ [1+ (y/n)] = ½ [1+ (181/589)] = 0.653650$
Now b=0.556876
As r = b, the message M = x = 67
So the Plaintext P = (M-Ks) = (67-24) = 43
So, the plaintext is successfully retrieved.

II. Results and Comparisons

We have compared the Modified Rabin Cryptosystem based on 3 parameters- Avalance Ratio, Non Homogeneity and Frequency Distribution. Both the table and the graph containing the compared values have been shown.

2.1 Avalanche Ratio

Avalanche Ratio shows how much modified the encrypted file is from the source file. It displays the ‘not same character percentage’, i.e. what percent of the characters in the encrypted file are not same as the source file. Here we have presented the avalance ratio of 15 files, encrypted by Rabin Cryptosystem, RSA and Modified Rabin Cryptosystem.

Table 1: Avalance Ratio of the files encrypted by Rabin, RSA and Modified Rabin

Sl No.	File Name	File Size	Avalance Ratio		
		(KB)	Rabin	RSA	Modified Rabin
1	Vande.txt	1.67	99.86	99.18	99.90
2	Cascade.css	1.75	99.75	99	99.75
3	Casarol.css	2.74	99.68	99.12	99.68
4	Boondh.txt	3.62	99.62	99.13	99.78
5	Windows.jpg	6.43	91.38	85.85	90.20
6	Hasnu.txt	7.76	99.87	97.30	99.87
7	Country.css	8.58	99.76	98.47	99.74
8	Bamboo.jpg	8.74	76.38	64.16	74.47
9	Bcpp.hlx	13	99.72	99.34	99.72
10	Justin.js	16.5	99.93	99.82	99.88
11	Jexpo.js	22.1	99.79	99.17	99.81
12	Durga.jpg	25	96.84	94.70	94.47
13	Ocf.hlx	31	99.96	99.75	99.98
14	Jri.js	38.7	99.82	99.81	99.78
15	Bcw.hlx	43	73.70	99.77	94.43

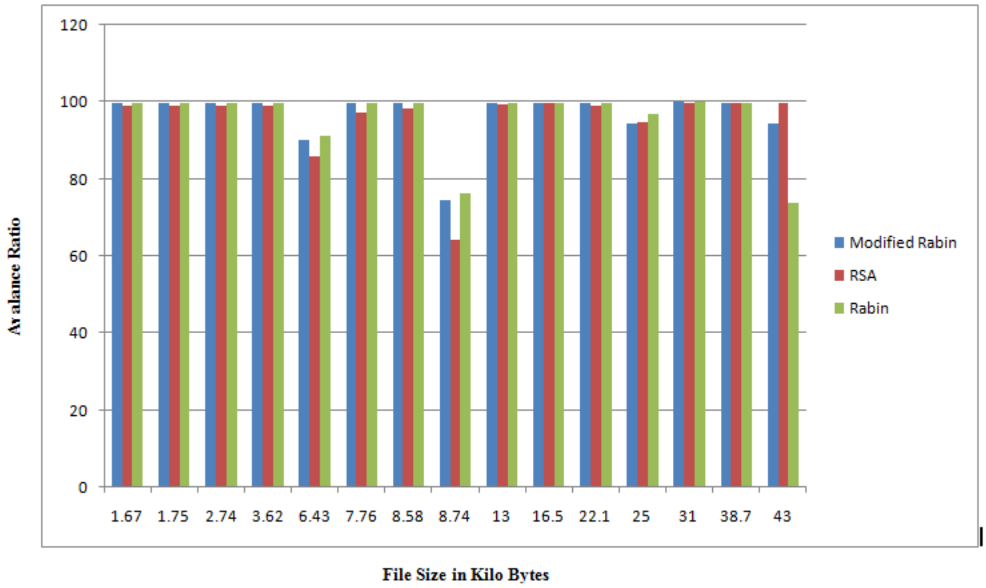
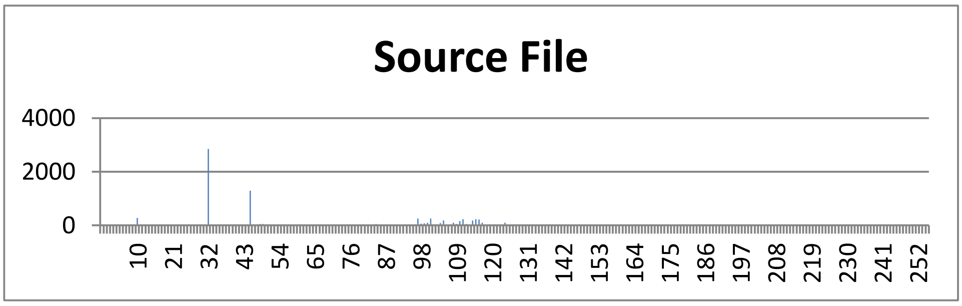


Fig. 3: Graph showing Avalance Ratio for Modified Rabin, RSA and Rabin Cryptosystem

Table 1 shows the Avalance Ratio for the files encrypted by Rabin Cryptosystem, RSA and Modified Rabin respectively. Fig.3 shows the Avalanche Graph for Modified Rabin, RSA and Rabin Cryptosystem respectively. As we can see, the Avalance Ratio of Modified Rabin Cryptosystem is better compared to the Rabin Cryptosystem and RSA cryptosystem. Except 2-3 files, most of the files display higher avalance ratio when encrypted by the Modified Rabin Cryptosystem.

2.2 Frequency Distribution

The variation of frequencies of all the 256 ASCII characters between the source file and the encrypted file are given in this section.



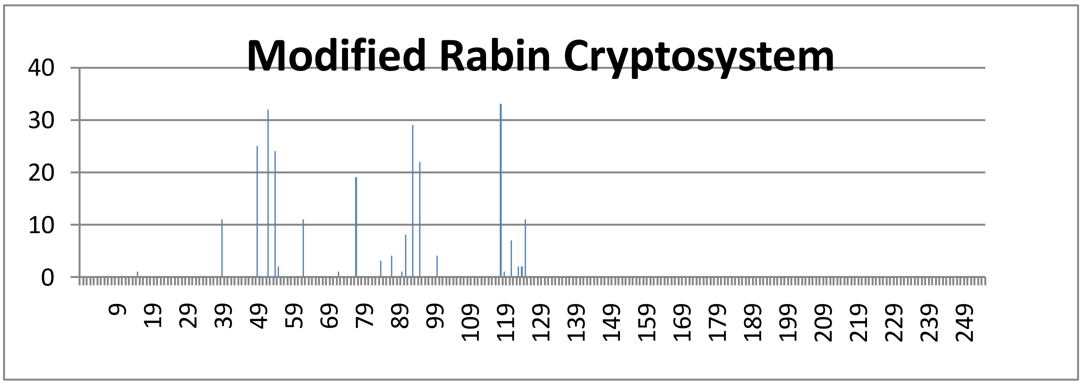


Fig 5: Frequency Distribution of ASCII characters in Modified Rabin Cryptosystem encrypted file

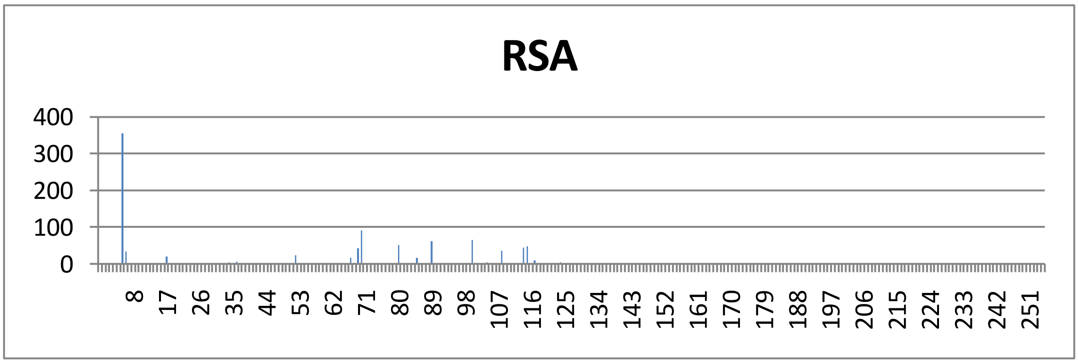


Fig 6: Frequency Distribution of ASCII characters in RSA encrypted file

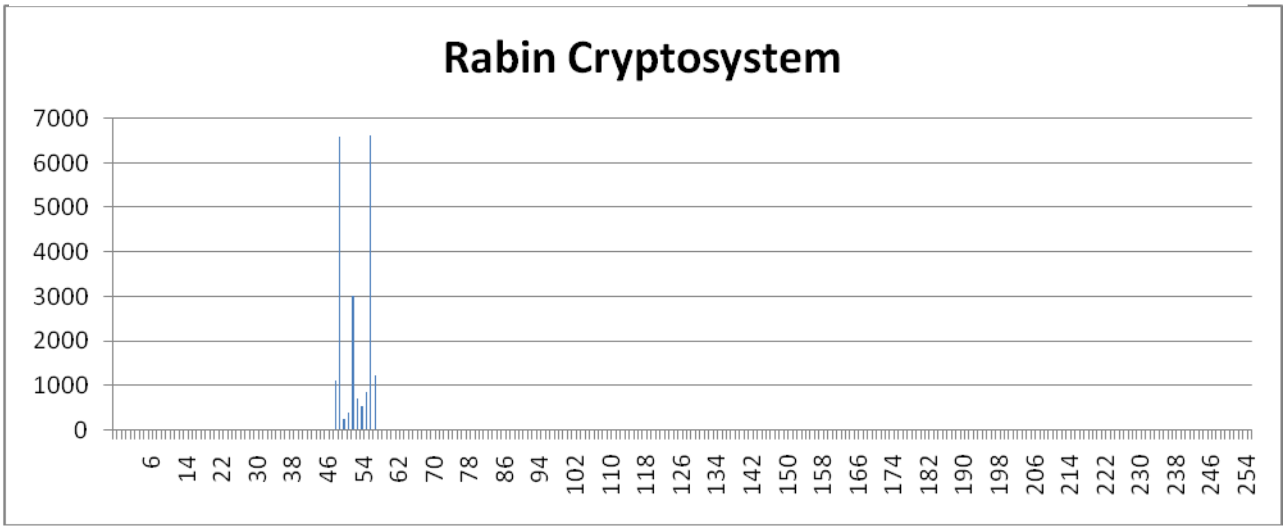


Fig 7: Frequency Distribution of ASCII characters in Rabin Cryptosystem encrypted file

Although 15 different files were encrypted and decrypted by the Modified Rabin Cryptosystem, Rabin Cryptosystem and RSA, only one such file is chosen here to analyze the frequency distribution of the characters. Figure 4, 5, 6 and 7 shows the frequency distribution of the source file, file encrypted by the Modified Rabin Cryptosystem, RSA and Rabin Cryptosystem respectively. A close observation reveals that, Modified Rabin Cryptosystem shows better frequency distribution of the ASCII characters throughout the character space, compared to the RSA and Rabin Cryptosystem.

2.3 Non Homogeneity Analysis

Another way in which we have analyzed the Modified Rabin Cryptosystem is by testing the homogeneity of the source and the encrypted file. For this purpose, we have performed the Chi-square test. Table 2 shows the File names, File size and corresponding Chi-square values and the Degree of Freedom for 15 different files encrypted by Rabin Cryptosystem, RSA and Modified Rabin respectively. Fig.8 shows the Chivalue graph of the same.

Table 2: Chi-square value and Degree of Freedom of 15 files encrypted by Rabin, RSA and Modified Rabin

Sl No.	File Name	File Size	Chivalue			Degree of Freedom		
		(KB)	Rabin	RSA	Modified Rabin	Rabin	RSA	Modified Rabin
1	Vande.txt	1.67	1563748	792494	326910	58	58	58
2	Cascade.css	1.75	480454	1283092	412927	67	67	67
3	Casarol.css	2.74	912135	597691	578580	71	71	71
4	Boondh.txt	3.62	1029324	3717	1842023	64	64	64
5	Windows.jpg	6.43	8291	6586	8003	255	255	255
6	Hasnu.txt	7.76	8669962	3751091	4066777	81	81	81
7	Country.css	8.58	3316237	2273058	1906523	68	68	68
8	Bamboo.jpg	8.74	21675	8954	8954	255	255	255
9	Bcpp.hlx	13	1550656	1889490	1920571	133	133	133
10	Justin.js	16.5	19712780	14122943	12035804	91	91	91
11	Jexpo.js	22.1	10884064	8661642	10379371	92	92	92
12	Durga.jpg	25	25325	26781	28776	255	255	255
13	Ocf.hlx	31	9370835	6989827	11583033	153	153	153
14	Jri.js	38.7	15941505	17645132	13715109	93	93	93
15	Bcw.hlx	43	1168395	1352432	2119305	164	164	164

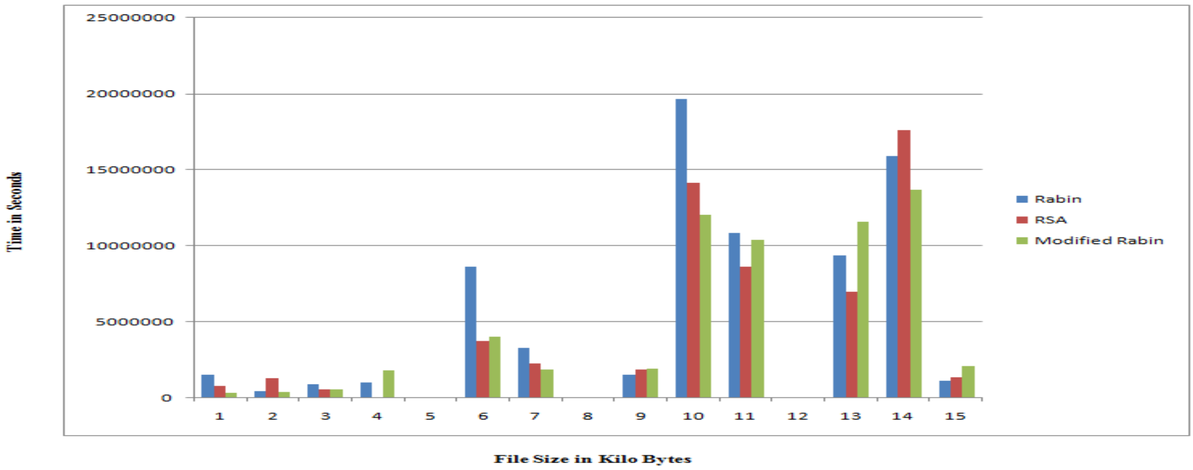


Fig.8: Graph showing the Chi square values of 15 files encrypted by Rabin, RSA and Modified Rabin

We can see that, barring some exceptions, the Chi-square values are increasing with the increase in file size. It is also noticed that Chi-square values of the Modified Rabin Cryptosystem are greater in most of the files compared to the RSA and Rabin Cryptosystem.

III. Contribution

Rabin Cryptosystem is an asymmetric cryptosystem, whose security is based on the hardness of factoring. The decryption function of the Rabin Cryptosystem is based on computing square roots modulo N. It is simple to compute square roots modulo a composite if the factorization is known, but very complex when the factorization is unknown. It is possible to prove that the hardness of breaking the Rabin Cryptosystem is equivalent to the hardness of factoring [1]. In this paper, we have modified the Rabin cryptosystem and have made it more secure, by converting the asymmetric Rabin Cryptosystem to a hybrid Cryptosystem. The key distribution scheme which is used before actual transaction is made between the sender and receiver ensures both confidentiality and authentication in the exchange of the secret key. This added secret key which can be renewed in each session and which is different between different pairs of users, adds more security to the Rabin cryptosystem. The decryption function of the Modified Rabin Cryptosystem is not only based on the hardness of factorization, it is also based on the shared secret key between the sender and the receiver. Even if 'N' is factorized, the original plaintext will not be retrieved without providing the secret key. Providing arbitrary random value in place of the actual secret key will only generate random garbage values, thus making the original plaintext harder to guess.

IV. Conclusion

The modified Rabin Cryptosystem suggested in this paper is a hybrid cryptosystem utilizing both the symmetric and asymmetric cryptosystem. The encryption function computes additional 2 values to be sent along with the cipher text to the receiver which helps in decryption process. In the decryption process Chinese Remainder Theorem is applied to get the 4 possible roots. Then the extra values received along with the cipher text and the shared secret key is needed to retrieve the original plaintext. The Modified Rabin Cryptosystem provides better security because of the addition of the shared secret key in both encryption and decryption procedure. The only disadvantage is that the initial transaction may take a bit long duration because of the key distribution process, though once the secret key is shared; the subsequent transactions in that session won't take that much time. Despite being a good alternative to the RSA cryptosystem, Rabin Cryptosystem is not so popular like RSA. After the modification suggested in this paper, we hope that Modified Rabin Cryptosystem fulfills all the requirements to be a good secure hybrid cryptosystem

.

Acknowledgement

The authors express their deep sense of gratitude to the Department of Computer Science and Engineering, Netaji Subhash Engineering College, West Bengal University of Technology.

References

Theses:

[1] Naiara Escudero Sanchez, *The Rabin Cryptosystem*. University of Paderborn

Books:

[2] W. Stallings, Cryptography and Network Security: *Principles and Practices* (Prentice Hall, Upper Saddle River, New Jersey, USA, Fifth Edition, 2011.)