© 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939

Hybrid Encryption Algorithm

[1]Gaurav R. Patel, [2]Prof. Krunal Panchal

[1]PG Scholar, [2]Assistant professor
LJIET, Ahmedabad
[1]gauravpatel9092@gmail.com

***Abstract* - Cryptography is derived from a Greek word which means, the art of protecting information by transforming it into an unreadable format. In order to prevent some unwanted users or people to get access to the data cryptography is needed. This paper introduces hybrid approaches by combining two most important algorithms RSA algorithm and Diffie Hellman algorithm. This hybrid encryption algorithm provides more security as compare to RSA algorithm. The implementation and result is also derived in the paper.**

***Key Terms* - RSA, Diffie-Hellman, Cryptography, Cryptosystem, private-key, public-key**

I. INTRODUCTION

Cryptography is a technique to hide the data over communication channel. It is an art to hide the data to strangers. As the technology grows day by day the need of data security over communication channel is increased to high extent. For securing the knowledge cryptography is use.

Symmetric key (also known as secrete-key cryptography) uses the only one key for both encryption and decryption. Any message which is encrypted by using the public key can only be decrypted by applying the same public key.

- Use a same key for to encrypt and to decrypt a message.
- Encryption and decryption algorithm is Different

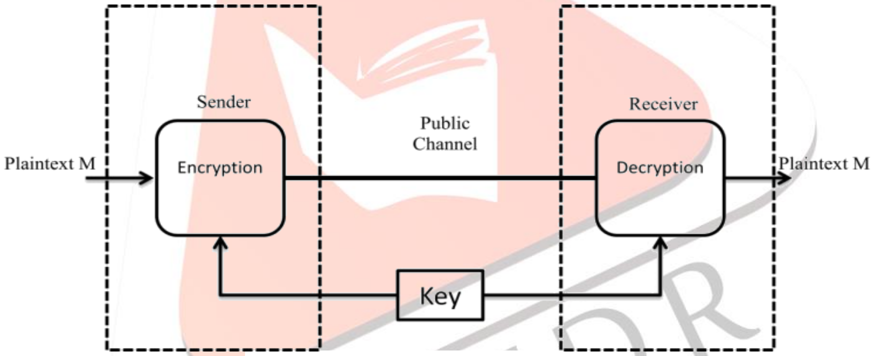


Figure1: Symmetric key Encryption

Asymmetric key (also known as public key encryption) uses two different keys to encryption and decryption of the message. The public key is made publicly available and can be used to encrypt messages. The private key is kept secret and can be used to decrypt received messages. RSA is asymmetric key encryption algorithm.

- Use a key (public key) to encrypt a message.
- Another (private key) to decrypt a message.

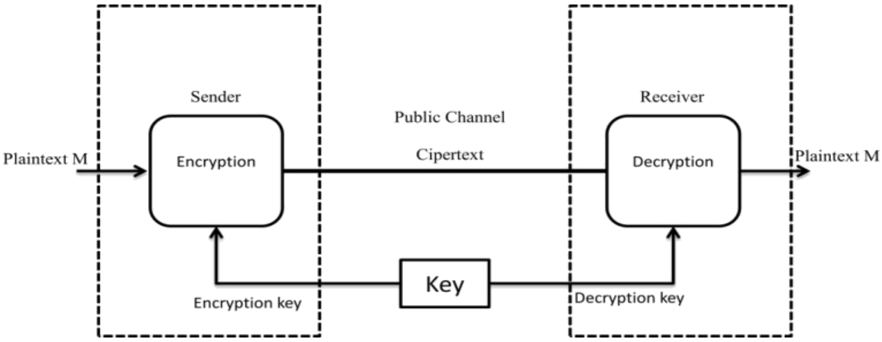


Figure2: Asymmetric key Encryption

II. RSA ALGORITHM

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. RSA formed the basis for a number of encryption programs. RSA is an algorithm for public key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It involves three steps: [2]

1. Key Generation,

2. Encryption And,
3. Decryption.

Phase 1: Key Generation

RSA involves two keys public key and private key. For encryption we use Public key and for decryption we use private key of message. The key generation takes places as follows [2]:

(a) Choose two distinct prime numbers P and Q
(b) Find N such that N= P*Q,
(c) Find the Phi of N, $\emptyset(N)$= (P-1)*(Q-1).
(d) Choose an E such that 1 < E < $\emptyset(N)$ and such that E and $\emptyset(N)$ share no Divisors other than 1 [E and $\emptyset(N)$ are relatively prime]. E is kept as the public key exponent.
(e) Determine D which satisfies the congruence relation.
E*D = 1 (mod $\emptyset(N)$).

Now, the public key consists of public key exponent E and N. And private key consists of private key exponent D & N.

Public Key: (E, N)
Private Key: (D, N)

Phase 2: Encryption

A process of converting Plain Text into Cipher Text is known as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure environment. The process of encryption requires two things- a key and an encryption algorithm. Encryption takes place at the sender side.

C = M ^ E mod (N)

Phase 3: Decryption

The process of converting Cipher Text into Plain Text is known as Decryption. Cryptography uses the decryption technique at the receiver side to convert the Cipher Text into original message. The process of decryption requires two things- a Decryption algorithm and a key.

M = C ^ D mod (N).

III. DIFFIE HELLMAN ALGORITHM

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. [7] Diffie–Hellman key exchange (D–H) is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. [13]

Diffie–Hellman is used by several protocols, including Secure Sockets Layer, Secure Shell, and Internet Protocol Security. Diffie–Hellman establishes a shared secret key that can be used for secret communications by exchanging data over a public network Steps of this algorithm are as:

[1] Select two numbers ‘R’ and ‘G’. ‘R’ is a prime number and ‘G’ is called as base.
[2] Select a secret number ‘A’ and another secret number ‘B’
[3] Calculate public number X = G^A mod R,
And Y = G^B mod R.
[4] Exchange their public numbers.
[5] Computes First session key as KA ,
KA= Y^A mod R
[6] Computes second session key as KB,
KB = X^B mod R
[7] Here KA = KB = K.

IV. PROPOSED HYBRID ALGORITHM

RSA and Diffie Hellman key exchange algorithm is widely used in now days. RSA algorithm is used for providing security of message using encryption and decryption process. The Diffie Hellman algorithm is used to generate the Secret key for the sender and receiver for communication. RSA algorithm provides more security as compared to other algorithm.

In this proposed model we add one more operation which is bitwise XOR operation. Because of this operation we can increase the complexity of the message. This operation is performed after the message is converted in to cipher text. In this proposed approach first we choose two prime numbers and find out the Encryption and decryption key exponents which will be used for encryption and decryption process. For Diffie Hellman algorithm we select A and B. R is a random prime number generated by the system automatically. The public number is generated by the Diffie Hellman algorithm. By using this public number we can generate secrete key KA and KB. This will be used to perform XOR operation.

At the sender side the encryption is done using encryption algorithm. When the encryption process completes XOR operation perform between cipher text and the first secrete key. After that operation the secrete message is sent over the medium.

At the receiver side the XOR operation is again performed between the second secret key and the secrete message which is sent by the sender. Using this operation we get the original cipher text. We can decrypt the cipher text using decryption algorithm and get the original message sent by the sender.

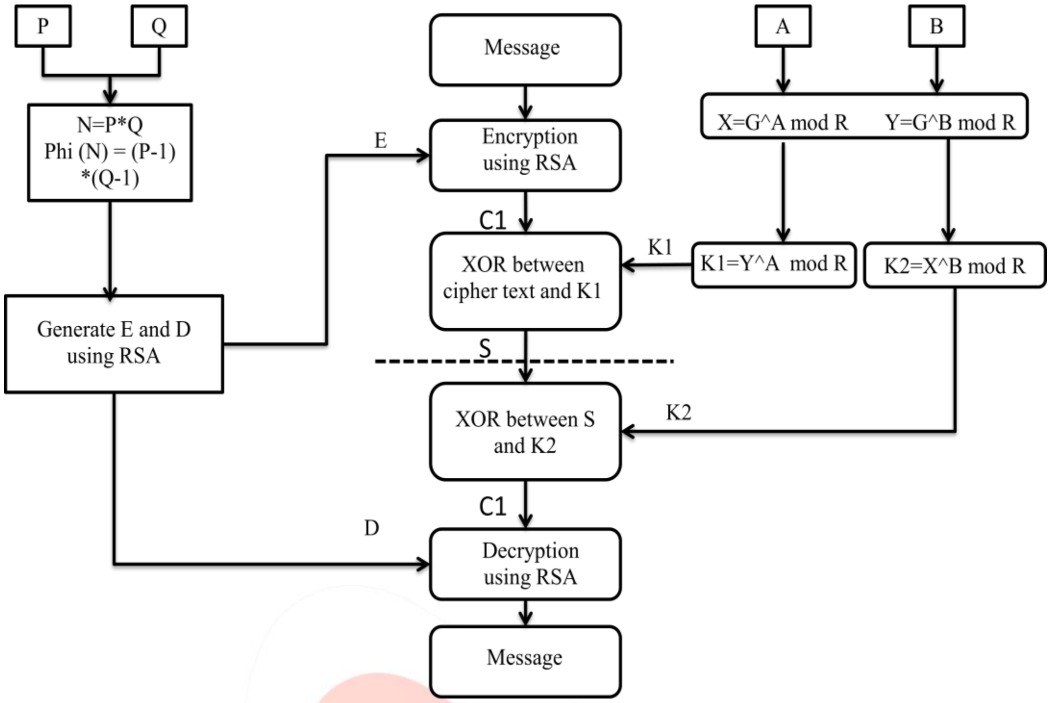


Figure 3: Proposed Model

In proposed model we take A and B as a random numbers. P, Q and R are prime numbers. G is integer number which is primitive root of R. C1 is cipher text and S1 is secret message. K1 and K2 is key generated by Diffie Hellman algorithm. E and D are encryption exponents and decryption exponents.

Following steps are performed by new proposed algorithm:
Step1: Choose two large prime numbers P and Q and random number A, B and G, R.
Step2: Set A and B for Diffie Hellman key generation
Step3: R and G are automatic generated constants.
Step4: Calculate N= P * Q.
Step5: Find Phi (N) = (P-1)*(Q-1)
Step6: Choose integer *E*, which can satisfy GCD [*E*, Φ (*N*)] =1. Φ (N. Where 1<E< Φ (N)
Step7: Calculate *D*, where E**D* = 1 mod Φ (*N*).
Step8: Now calculate following as public number
Calculate X= G^A mod R, Y= G^B mod R
Step9: Secret key K1 = Y^A mod R,
K2 = X^B mod R.
Step10: Encrypt message using RSA algorithm,
C1= (M ^ E) mod N.
Step11: X-OR between C1 and key K1,
S= C1⊕ K1
Step12: At receiver side X-OR is between S and
Key K2, C1= S ⊕ K2.
Step13: Decrypt message using RSA algorithm
M= (C1^ D) mod N.

Example:

Let us consider that, we have to send a message whose value is 88 i.e. m=88.
Step1: Choose P=11 and Q=17 and
Random number A=5, B=6 and
G=2, R=997.
Step2: N = 11 x 17= 187
Step3: Phi (N) = (11-1) (17-1) = 160
Step4: Now calculate following as public number
Calculate X= 2^5 mod 997 =32,
Y= 2^6 mod 997 = 64
Step5: K1 = 64^5 mod 997=740
K2 = 32^6 mod 997= 740
Step6: Choose integer *E*, E=7
Step7: 7**D* = 1 mod Φ (*N*). D= 23

Step8: Encryption

$C1= (88 \wedge 7) \bmod 187 = 11$

Step9: X-OR between C1 and key k1

$S= C1 \oplus K1 = 11 \oplus 740 = 751$

Step10: At receiver side $C1= S \oplus K2$

$C1= 740 \oplus 751 = 11$

Step11: Decryption

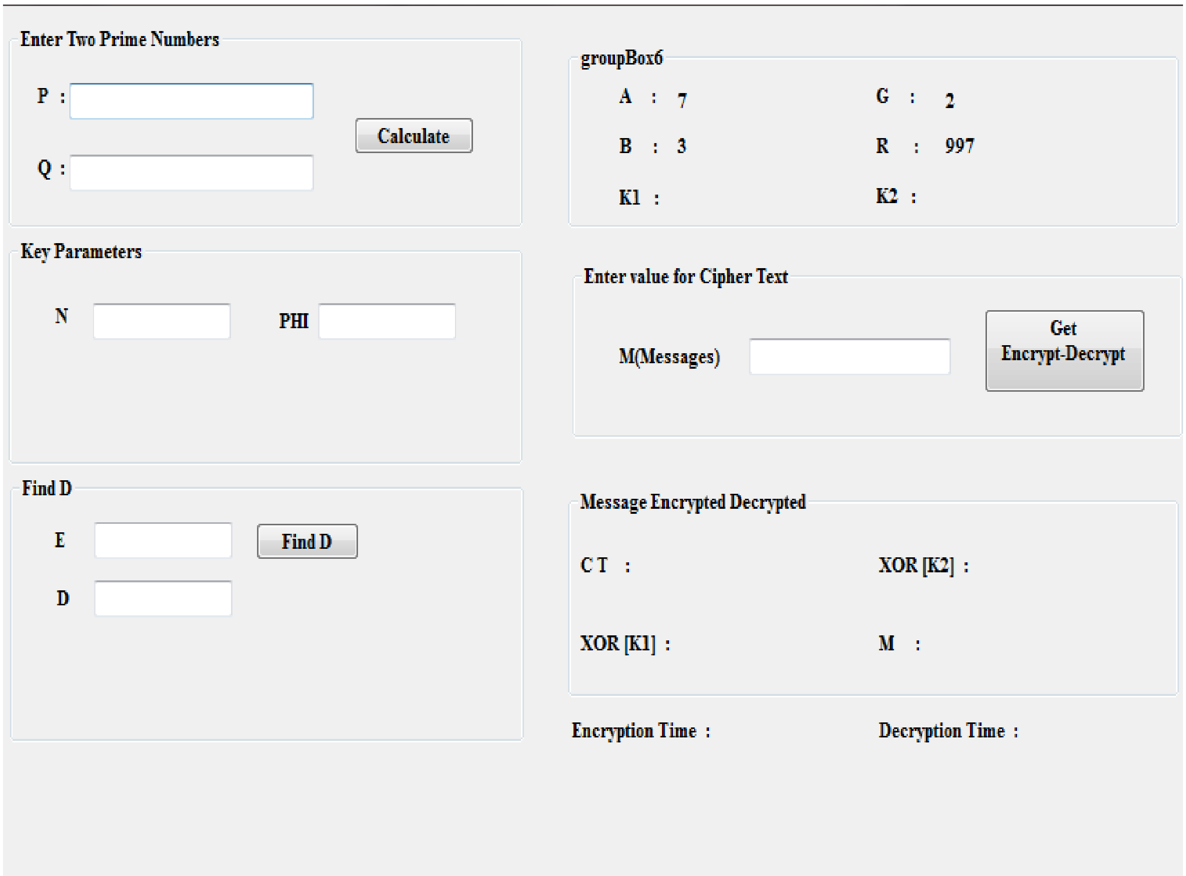
$M= (11 \wedge 23) \bmod 187 = 88$

V. IMPLEMANTION

NET Framework (Known as dot *net*), a software framework which is developed by Microsoft that runs primarily on Microsoft Windows. It provides language interoperability across several programming languages.NET Framework includes a large library.

.NET Framework's Framework Class Library provides user interface, data-access, database connectivity, cryptography, web-application development, numeric algorithms, and network communications. Programmers produce software by combining their own source with .NET Framework and other libraries. .NET Framework is intended to be used by most new applications created for the Windows platform. Microsoft also produces an integrated development environment largely for .NET software called Visual Studio. [12]

The GUI was developed using Microsoft asp.net frame work. The programming language is c#. It provide option to choose user define prime number and the also user can input the message which is sent from sender to receiver.



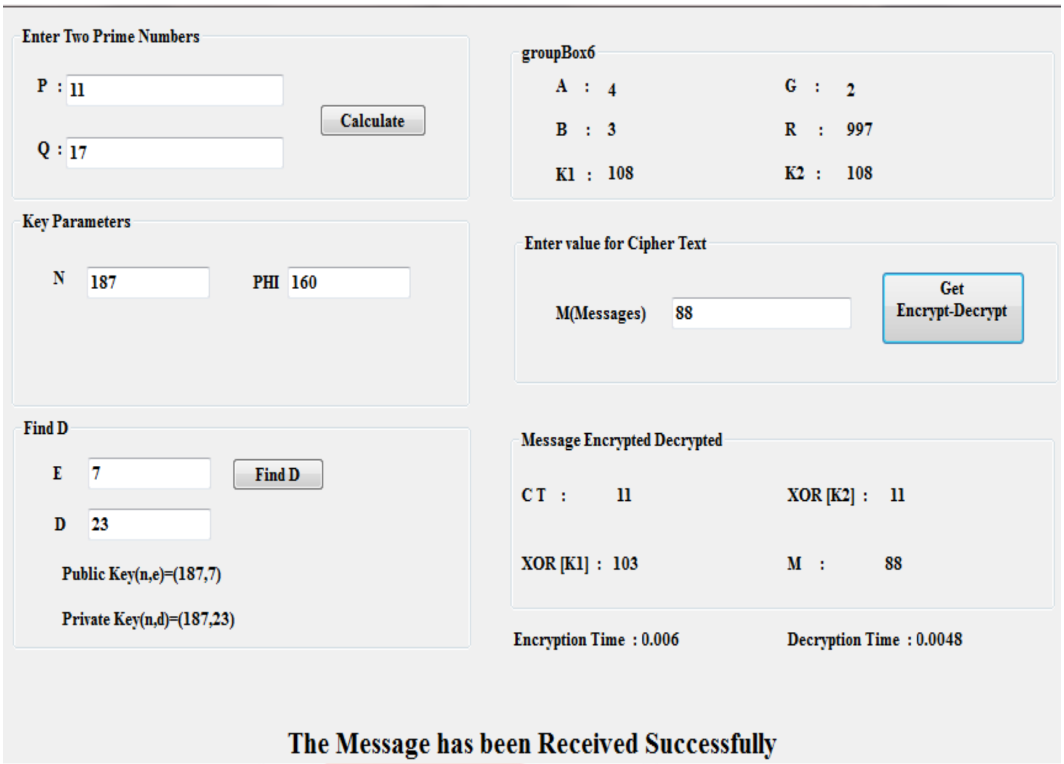
A : 7

G : 2

B : 3

R : 997

Figure 4: GUI View of proposed model



Enter Two Prime Numbers

P : 11

Q : 17

groupBox6

A : 4 G : 2

B : 3 R : 997

K1 : 108 K2 : 108

Key Parameters

N 187 PHI 160

Enter value for Cipher Text

M(Messages) 88

Find D

E 7

D 23

Public Key(n,e)=(187,7)

Private Key(n,d)=(187,23)

Message Encrypted Decrypted

C T : 11 XOR [K2] : 11

XOR [K1] : 103 M : 88

Encryption Time : 0.006 Decryption Time : 0.0048

The Message has been Received Successfully

Figure 5: Encryption and Decryption of message

VI. RESULT

Encryption and Decryption Time Comparison:

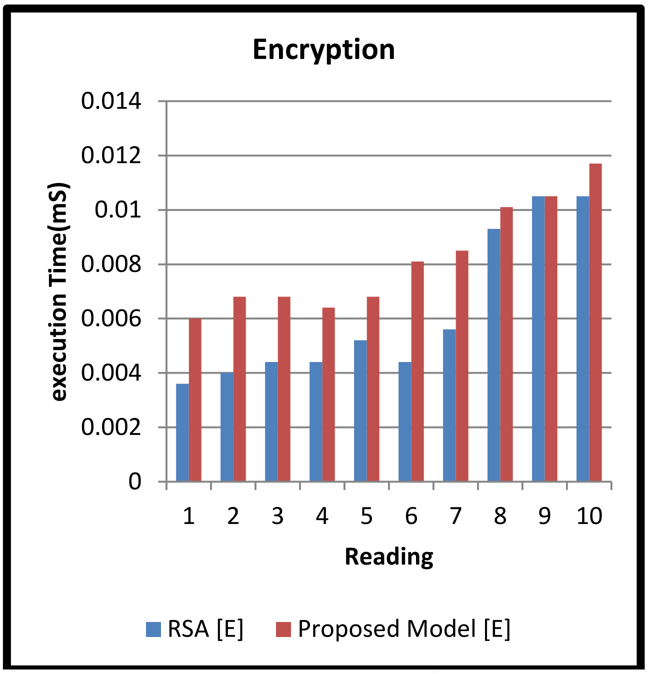
Table 1 and table 2 shows the encryption time and decryption time for the standard RSA algorithm and proposed model.

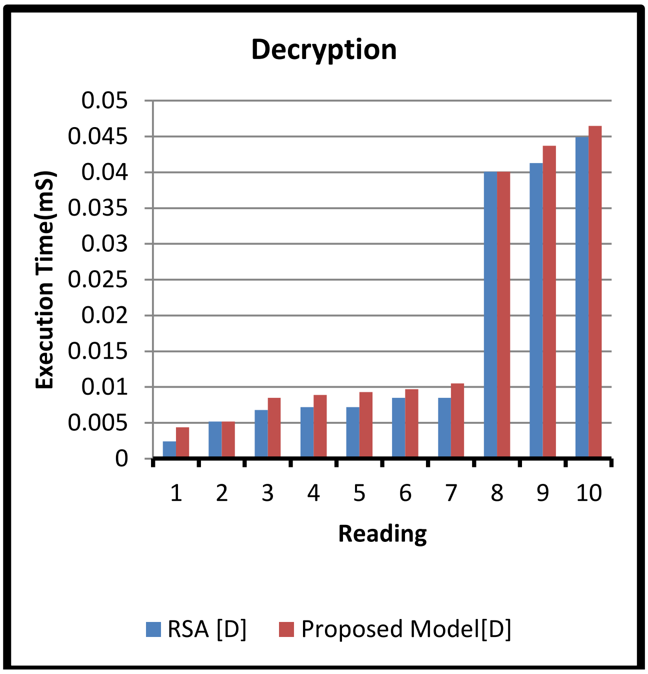
Standard RSA model					
P	Q	E	D	E [MS]	D [MS]
11	17	7	23	0.0036	0.0024
401	277	7	31543	0.0040	0.0052
1447	941	7	1165063	0.0044	0.0068
5693	5791	7	28248583	0.0044	0.0072
6917	6997	5	38707469	0.0052	0.0072
23899	23909	5	114270677	0.0044	0.0085
36037	36017	5	1038298061	0.0056	0.0085
215981	215983	7	39983822023	0.0093	0.0401
317263	317267	5	40262578277	0.0105	0.0413
532093	532099	5	226500071213	0.0105	0.0449

Table 1: encryption and decryption time for RSA

Proposed model					
P	Q	E	D	E [MS]	D [MS]
11	17	7	23	0.0060	0.0044
401	277	7	31543	0.0068	0.0052
1447	941	7	1165063	0.0068	0.0085
5693	5791	7	28248583	0.0064	0.0089
6917	6997	5	38707469	0.0068	0.0093
23899	23909	5	114270677	0.0081	0.0097
36037	36017	5	1038298061	0.0085	0.0105
215981	215983	7	39983822023	0.0101	0.0401
317263	317267	5	40262578277	0.0105	0.0437
532093	532099	5	226500071213	0.0117	0.0465

Table 2: encryption and decryption time for proposed model



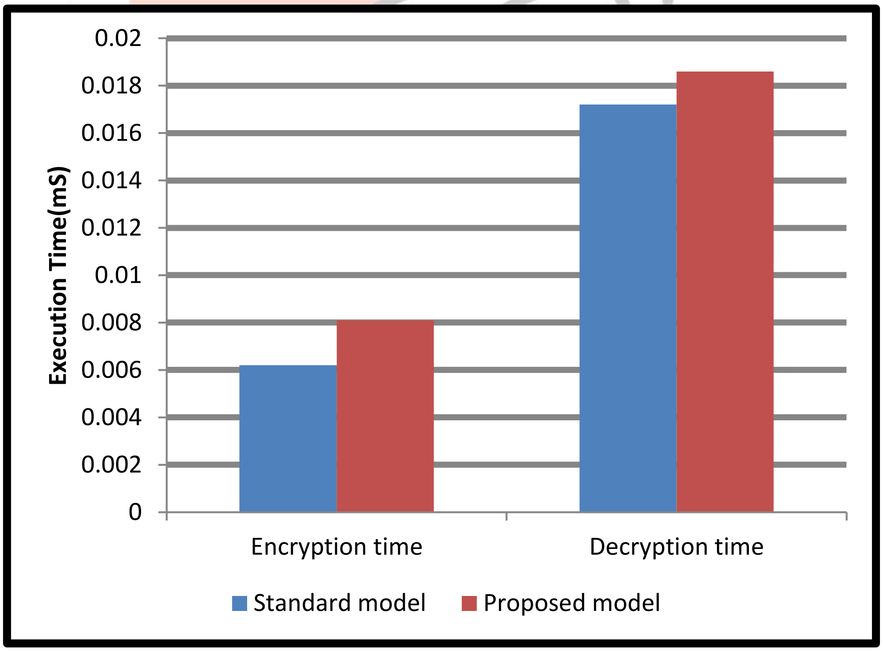


The graph shows the encryption time and decryption time comparison for the standard RSA model and proposed model.

Average time	Standard Model	Proposed model
Encryption time	0.0062	0.0081
Decryption time	0.0172	0.0186
Total time	0.0234	0.0267

Table 3: Time comparison

Table 3 shows the average time of encryption and decryption process for reading which is shown in table 1 and table 2. It also calculated the total execution time for the standard RSA algorithm and proposed model.



The graph shows comparison of total time between standard RSA model and new proposed model. When comparing with RSA, proposed model requires more time for encryption and decryption. Whereas proposed model is more secured cryptography algorithm than RSA, because proposed model includes X-or concept, which is more difficult for the intruder to find the plain text from the secrete message.

VII. CONCLUSION

In proposed hybrid encryption algorithm we can improve security of message by combining encryption and bitwise x-or operation because of this operation the complexity of the message is also increased. The new proposed model provides more security compared to normal RSA algorithm.

REFERENCES

[1] William Stallings, ‘Cryptography and Network Security’, ISBN 81-7758-011-6, Pearson Education, Third Edition

[2] Al-Hamami, A. H., & Aldariseh, I. A. (2012, November). Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). IEEE.

[3] Chhabra, A., & Mathur, S. (2011, October). Modified RSA Algorithm: A Secure Approach. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on (pp. 545-548). IEEE.

[4] Sun, Hung-Min, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek. ‘Dual RSA and its security analysis.’ Information Theory, IEEE Transactions on 53, no. 8 (2007): 2922-2933.

[5] Dhakar, R. S., Gupta, A. K., & Sharma, P. (2012, January). Modified RSA Encryption Algorithm (MREA). In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on (pp. 426-429). IEEE.

[6] Wang Rui; Chen Ju; Duan Guangwen, ‘A k-RSA algorithm,’ Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.21,24, 27-29 May 2011

[7] Gupta, S., & Sharma, J. A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman.

[8] Garg, V., & Rishu, R. (2012). Improved Diffie-Hellman Algorithm for Network Security Enhancement. International Journal of Computer Technology and Applications, 3(4).

[9] TT II, C. C. H. H. A. A. R. R., and CCLL EE. ‘Analysis Improved Cryptosystem Using DES with RSA

[10] Kaur, Khushdeep, and Er Seema. ‘Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices.’ International Journal of Engineering Research and Applications (IJERA) 2.5 (2012): 914-917

[11] Pugila, Dhananjay, Harsh Chitrala, Salpesh Lunawat, and PM Durai Raj Vincent. ‘AN EFFICEIENT ENCRPYTION ALGORITHM BASED ON PUBLIC KEY CRYPTOGRAPHY.’ International Journal of Engineering and Technology (2013).

[12] http://en.wikipedia.org/wiki/.NET_Framework

[13] http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange