Compresive Anyalsis of RSA Algoritham

Vikram Solanki
LJIET
Department of Computer Engineering
Ahmedabad, India

Abstract*—RSA algorithm is windy use now days.RSA algorithm provides higher security as compared to other algorithm. In my previous paper we proposed a new model with XOR operation which provide more complexity during encryption and decryption process.IN this paper we analysis the rsa algorithm hybrid encryption algorithm and our proposed algorithm.

Keywords*— RSA, diffi-helman, encryption, decryption, public key, private key

I. 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. There are mainly three steps in RSA algorithm: [2]

1) *Key Generation*
2) *Encryption algorithm*
3) *Decryption algorithm*

Phase 1: Key Generation

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

(a) Select two prime numbers P and Q

(b) Select N such that N= P*Q,

(c) Find, where = (P-1)*(Q-1).

(d) Choose an E such that 1 < E < and such that E and share no Divisors other than 1. E is kept as the public key exponent.

(e) Determine D where, E*D = 1 (mod).

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 simple Text into Cipher Text is called as Encryption process. We can use 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 called as Decryption. This revert process of encryption is known as Decryption. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. M = C ^ D mod (N).

II. HYBRID ENCRYPTION USING RSA AND DIFFIE-HELLMAN

Shilpi Gupta and Jaya introduce new concept using two most important algorithm RSA and Diffie-Hellman. RSA and Diffie Hellman both algorithm are combined and proposed new algorithm. The RSA algorithm is be used for public key encryption and digital signature. In this approach the RSA algorithm is used for generation of key. Using RSA we can get public and private key for encryption and decryption process. Diffie Hallman algorithm is used as key exchange method that allows two parties that have no prior knowledge to each other to jointly share a secret key. In this approach the RSA keys were taken as input for Diffie Hellman. The keys are generated using public and private key of RSA algorithm. The Diffie Hallman is used for generating more secure cipher text. For encryption XOR operation is performed between plaintext and key generated by Diffie Hellman algorithm. For decryption process XOR operation is performed between cipher text and key. It will be easy for user to send and receive messages and files which are the most confidential for user. [7]

III. PROPOSED HYBRID 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 two random numbers which is number 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.

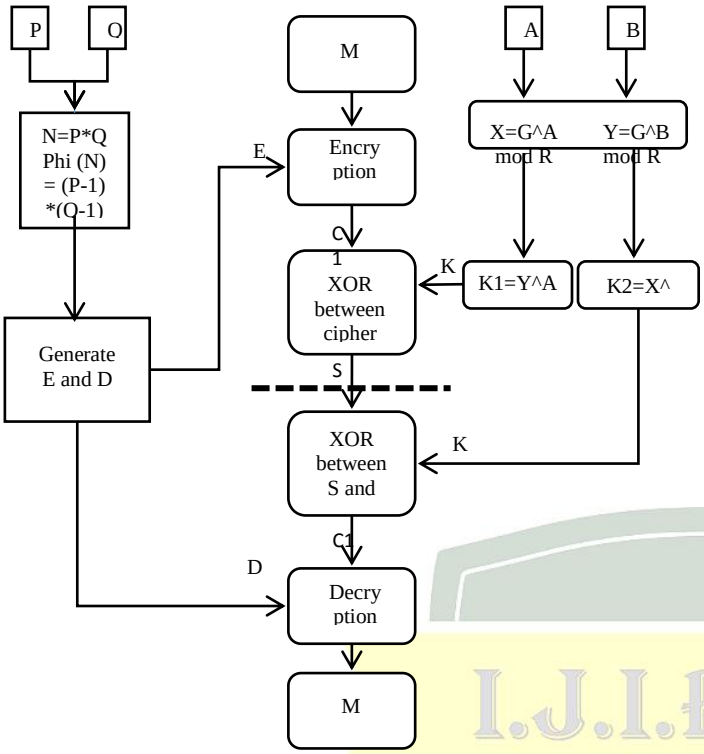


Figure 1: Proposed Model

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.

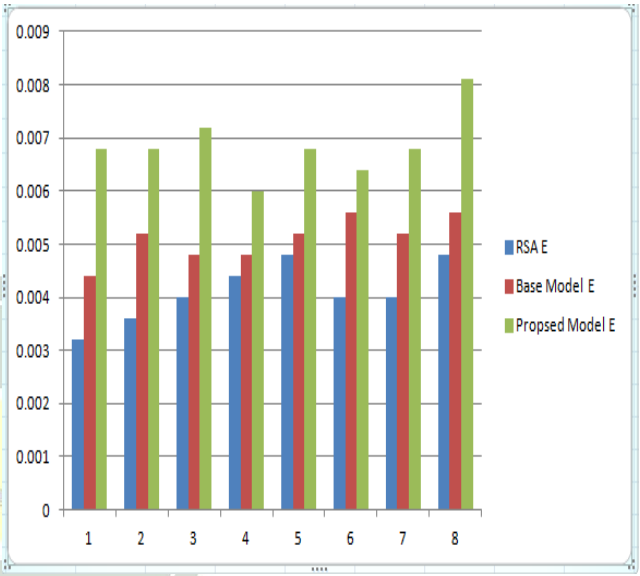
IV. ANALYSIS AND COMPARISON

Now we deeply analysis the model and compare then result for encryption and decryption process. Let's take two prime numbers. P=9976 and q=9973. We will set p and q constant and take the reading of the encryption time and decryption time for following three models. 1) Standard rsa model 2) base paper model 3) proposed model.

Rsa model		Base model		Proposed model	
En	De	En	De	En	De
0.0032	0.0068	0.0044	0.0020	0.0068	0.0076
0.0036	0.0081	0.0052	0.0024	0.0068	0.0097
0.0040	0.0081	0.0048	0.0024	0.0072	0.0097
0.0044	0.0081	0.0048	0.0020	0.0060	0.0101
0.0048	0.0081	0.0052	0.0024	0.0068	0.0105
0.0040	0.0093	0.0056	0.0024	0.0064	0.0121
0.0040	0.0081	0.0052	0.0020	0.0068	0.0101
0.0048	0.0085	0.0056	0.0020	0.0081	0.0097

Table 1: Time comparison for Encryption & Decryption

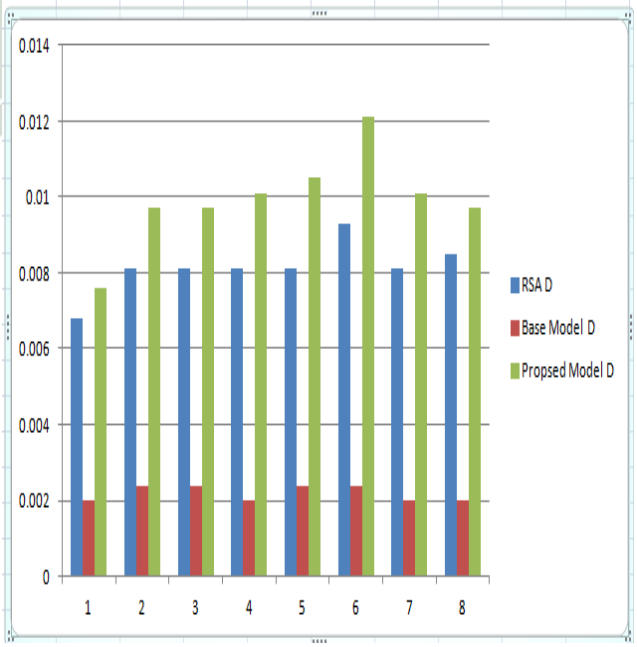
Encryption time comparisons



X-axis - reading, y-axis - execution time (ms)

Graph1: encryption time comparisons

Decryption time comparisons



X-axis - reading, y-axis - execution time (ms)

Graph2: decryption time comparisons

Let's take two prime numbers. P= 15307 and q=15319. We will set p and q constant and take the note the encryption time and decryption time for following three models.

1) Standard RSA model

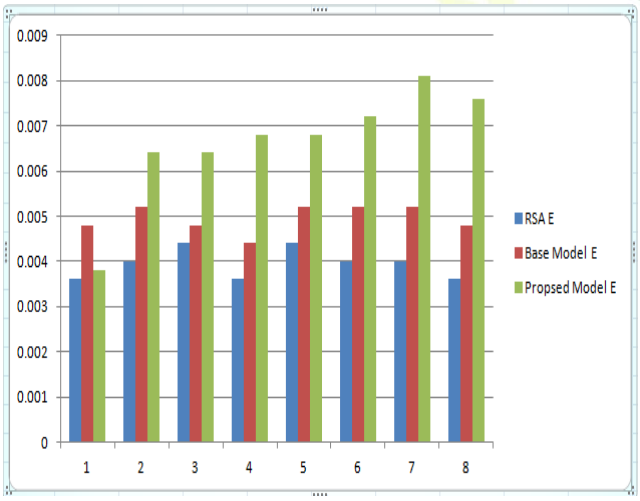
2) Base paper model

3) Proposed model

Rsa model		Base model		Proposed model	
En	De	En	De	En	De
0.0036	0.0085	0.0048	0.0024	0.0038	0.0081
0.0040	0.0085	0.0052	0.0020	0.0064	0.0081
0.0044	0.0081	0.0048	0.0020	0.0064	0.0093
0.0036	0.0081	0.0044	0.0024	0.0068	0.0097
0.0044	0.0081	0.0052	0.0020	0.0068	0.0093
0.0040	0.0081	0.0052	0.0016	0.0072	0.0105
0.0040	0.0076	0.0052	0.0020	0.0081	0.0101
0.0036	0.0081	0.0048	0.0032	0.0076	0.0093

Table 3: Time comparison for Encryption & Decryption

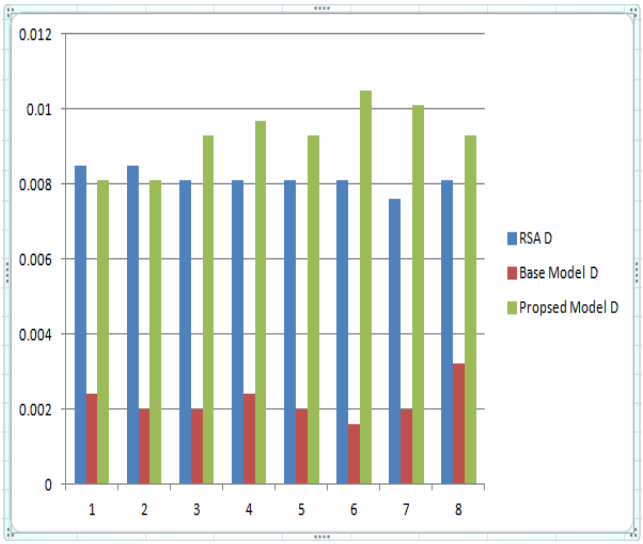
Encryption time comparisons



X-axis - reading, y-axis - execution time (ms)

Graph3: encryption time comparisons

Decryption time comparisons



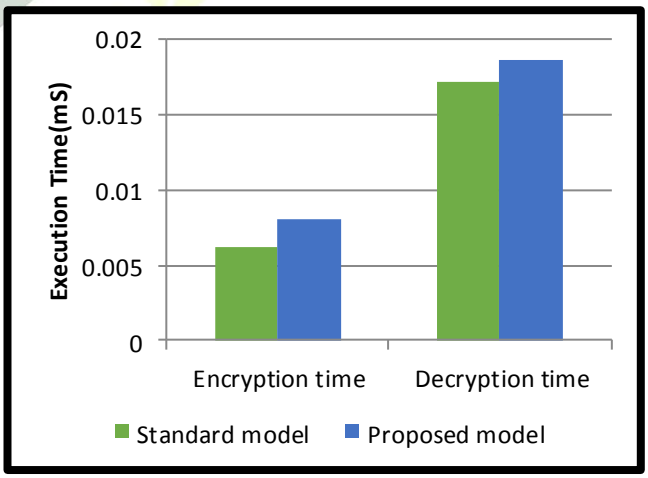
X-axis - reading, y-axis - execution time (ms)

Graph4: decryption time comparisons

Time comparison between models:

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 1: Average time comparison for Encryption & Decryption



Graph5: decryption time comparisons

The graph displays the time comparison for rsa model and new projected model. As compared to rsa model proposed model takes longer time decipherment however, it's a lot

of secured than rsa as a result of proposed model includes x-or conception, that is tougher for the trespasser to seek out the plain text from the secrete message.

REFERENCES

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

[2] http://en.wikipedia.org/wiki/RSA_(cryptosystem)

[3] 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.

[4] 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.

[5] 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.

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

[9] Nagar, Sami A., and Saad Alshamma. "High speed implementation of RSA algorithm with modified keys exchange." Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on. IEEE, 2012.

[10] 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).

[11] Ivy, B. Persis Urbana, and Purshotam Mandiwa Mukesh Kumar. "A modified RSA cryptosystem based on 'n'prime numbers."