Hybrid Public Key Cryptosystem Combining RSA & DES Algorithms

Saba Khanum
Department of Information Technology
Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi, India

Bharti Sharma
Department of Computer Science and Engineering
Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi, India

Gunjan Beniwal
Department of Computer Science and Engineering
Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi, India

Abstract- Public Key Cryptosystem is used for high authenticity and security of transmitted messages. In public key cryptosystems, the sender and receiver both have two different keys used for encryption and decryption.In the proposed algorithm, the RSA algorithm proposed by Rivest et al has been modified using four large 64 bit prime numbers instead of two as in traditional RSA algorithm. In the modified RSA, the security of the algorithm has been increased exponentially by increasing the factors used in Euler's Totient Function[1]. Instead of two prime factors present in the traditional RSA, four Big Integer type random prime numbers are used in the HYBRID RSA-DES algorithm. This provides additional security against brute force attacks.The proposed algorithm has been further modified by creating a new hybrid using the DES or Data Encryption Standard algorithm. The random number generated by the GCD of Euler's Totient Function along with one is enhanced and modified using the permutation tables from DES algorithms. In the 64 bit key e, every 8th bit is discarded and the matrices of remaining 56 bits are subjected to Compression Permutation from the DES algorithm. These compression permutations generate a modified 48 bit key. This key is subjected to a series of 8 S-BOX Substitutions which give a 64 bit modified key. This key is then modified using a Final Permutation to generate a 64 bit modified and highly secure key.The Hybrid algorithm is then compared with various other algorithms like RSA, Modified RSA and DES. The results are plotted in a graph. The time complexity for all the algorithms is compared and the Hybrid algorithm provides least time for encryption and decryption.The used algorithms are implemented and the results are compared. As the size of keys increases, the time complexity and security of the Hybrid Algorithm are found to be increased.
Keywords – Public key Cryptosystem, RSA, Time Complexity

I. INTRODUCTION

A.studied algorithms-rsa public key cryptosystem [2] [3][4]
[5]a cryptography system has 3 main parts:-

- Operations involved in converting plain text to cypher text.
- Method of processing plain text
- No of encryption/decryption keys used.

[6]In public key cryptography system, there are different set of keys for both sender and receiver unlike private key cryptography algorithms which have only one same key both for the sender and the receiver.
The important components of a public key cryptosystem are:-

- Plain Text
- Encryption Algorithm
- Public Key
- Private Key
- Decryption Algorithm
- Cypher Text

In traditional RSA algorithm, two prime numbers are used to generate a public key for encrypting the text. This key is given to user. By using this key a decryption key can be generated to decipher the cypher text into plain text.The problem with traditional RSA is that using brute force attacks, the prime numbers can be detected making the algorithm prone to attacks. In further given algorithms, the key generation mechanisms have become more complex so that the security of the algorithms can be increased exponentially.
The RSA algorithm is given below.

RSA ALGORITHM [7]

INPUT
Two 64 bit prime numbers

OUTPUT
Public Key Components: {e, n}
Private Key Components: {d, n}

PROCEDURE
$N = p*q$
$\Phi(n) = (p-1)(q-1)$

Find random number e, such that,
- $1 < e < \Phi(n)$
- $GCD(e, \Phi(n)) = 1$

$d = e^{-1} \bmod(\Phi(n))$

ENCRYPTION
Enter a message M such that, M<n
Cypher Text, $C = M^e \bmod n$

OUTPUT: - C

DECRYPTION
Plain text, $P = C^e \bmod n$

OUTPUT: - M

(a)

MODIFIED RSA ALGORITHM

INPUT
Four 64 bit prime numbers p, q, y and z

OUTPUT
Public Key Components: {e,n}
Private Key Components: {d,n}

PROCEDURE
$N = p*q*y*z$
$\Phi(n) = (p-1)*(q-1)*(y-1)*(z-1)$

Find random number e, such that,
- $1 < e < \Phi(n)$
- $GCD(e, \Phi(n)) = 1$

$d = e^{-1} \bmod(\Phi(n))$

ENCRYPTION
Enter a message M, such that, M<n
Cypher Text, $C = M^e \bmod n$

OUTPUT: - C

DECRYPTION
Plain text, $P = C^e \bmod n$

OUTPUT: - M

OUTPUT: - M

(b)

Figure 1: (a)Showing present RSA algorithm (b) Modified RSA algorithm

B.Modified Rsa Public Key Cryptosystem [8] [9]

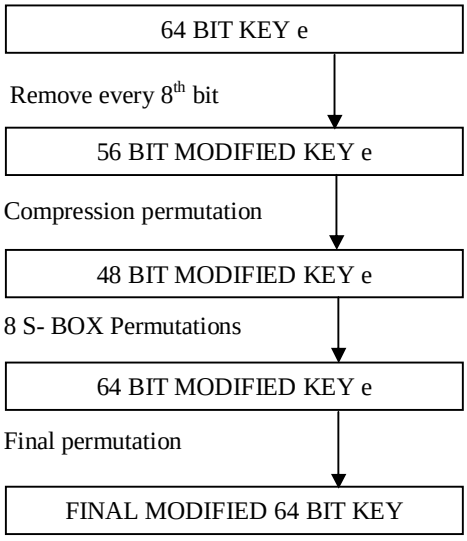
In this algorithm given by M. Thangavel et al in the paper An Enhanced and Secured RSA Key Generation Scheme (ESRKGS), four prime numbers have been used instead of instead of two prime numbers to calculate N which makes the system highly secure as it is possible only to find p and q with existing factorizing techniques. Thus making the system difficult to break.The values of e and d depend on N, which is a multiple of four prime numbers. Also the value of e is not computed directly. It is computed using the values of e1 and e2 which increases the time taken to break the system. Also all four prime numbers cannot be easily guessed if the value of N is known. The bit length of all the prime numbers chosen is same as in traditional RSA.

II.PROPOSED ALGORITHM

Hybrid Rsa-Des Algorithm

In this algorithm, an attempt has been made to combine the Modified RSA and DES algorithm to increase the security of the traditional RSA against brute force attacks.The following modifications have been made in the HYBRID RSA-DES algorithm:-

- Instead of two prime numbers in traditional RSA, four prime numbers have been used.
- [10]Once the key is generated, Initial Permutations have been used to transform the key.
- The 8 S-BOX substitution boxes have been used from traditional DES to transform the HYBRID algorithm key using XOR transformations.
- Then final permutation of 64 bit Encrypted Block is used from DES to give a transformed new value of the key.
- The new key is used to Encrypt and Decrypt the messages from sender to receiver.



Implementation Of Hybrid Rsa -Des Algorithm

INPUT
Four 64 bit prime numbers p, q, y and z

OUTPUT
Public Key Components: {e, n}
Private Key Components: {d, n}

PROCEDURE
$N = p*q*y*z$
$\Phi(n) = (p-1)*(q-1)*(y-1)*(z-1)$
Find random number e, such that,
- $1 < e < \Phi(n)$
- $GCD(e, \Phi(n)) = 1$

Once the64 bit key, e is obtained, the following transformations have been applied on the key.

- Discarding of every 8th bit in the key, e.

1	2	3	4	5	6	7	8	9	10	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	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

- After key transformations, 48 of the 56 bits are selected using the following COMPRESSION PERMUTATIONS have been used to transform the HYBRID ALGORITHM KEY.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

- Then S-BOX Substitutions have been used to perform S-box 1 to S- box 8 permutations from traditional DES TO transform the 48 bit key into different complex permutations of 64 bits.

- Then a final permutation is performed to generate a 64 bit key which is used in Encryption and Decryption.

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	21	9	49	17	57	25

The new generated modified key is used in the given formulas.
$d = e^{-1} \bmod(\Phi(n))$

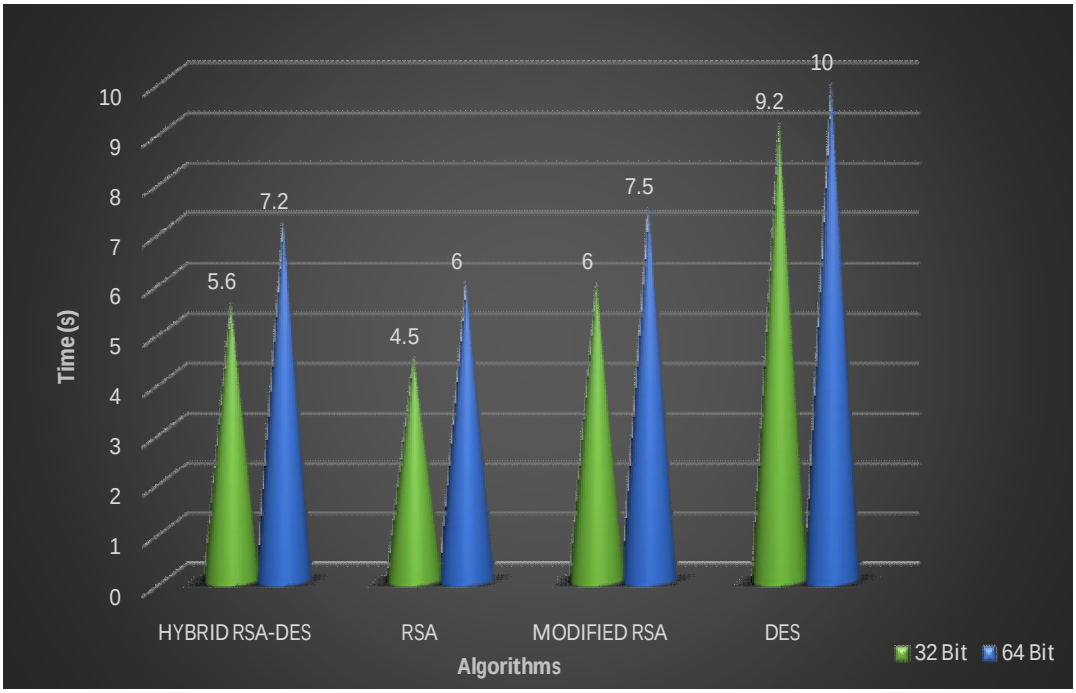
ENCRYPTION
Enter a message M, such that, $M<n$
Cypher Text, $C = M^e \bmod n$

OUTPUT: - C

DECRYPTION
Plain text, $P = C^e \bmod n$

OUTPUT: - M

III.COMPARISION BETWEEN HYBRID RSA, MODIFIED RSA, TRADITIONAL RSA AND DES ALGORITHMS



This graph depicts the comparison between the four implemented algorithms namely: hybrid rsa, modified rsa, traditional rsa and des. The data is taken over 32 bit and 64 bit public keys. The time variation is shown on y-axis while the x-axis denotes the corresponding algorithms.

IV.CONCLUSION

Various traditional algorithms like RSA, Modified RSA and DES have been studied and implemented and a Hybrid RSA-DES Algorithm has been created. The results show that the time complexity of the proposed algorithm is less than the pre-existing algorithms. The new proposed algorithm provides better efficiency for encryption and decryption.Hybrid RSA-DES Algorithm uses four prime numbers for calculating the value of N, hence the prime factorization of N cannot be easily performed using Brute Force. The public key generated is subjected to various permutation tables from traditional DES namely: Compression Permutation, 8 S-BOX Permutations and Final Expansion Permutation. This generated modified 64-bit key which enhances the security of the algorithm.The key is then used to perform encryption and then the private key generated is used for decryption.The new algorithm provides better results than other algorithms.

V.FUTURE WORK

The following enhancements can be made in the given algorithm:-

- Support for higher bit message and key
- Character and special symbol support in message
- Improve security by increasing parameters
- Increase efficiency
- Adding and implementing further algorithms to add new security features to the algorithm.

REFERENCE

[1] http://www.whitman.edu/mathematics/h igher_math_online/section03.08.html
[2] Data Communications & Networking , Behrouz Forouzan Tata McGraw-Hill Education, 2006 - Computer networks
[3] Gaines, H. F. (2014). *Cryptanalysis: A study of ciphers and their solution*. Courier Corporation.
[4] http://searchsecurity.techtarget.com/RSA
[5] Diffie, W., & Hellman, M. E. (1979). Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, *67*(3), 397-427.
[6] http://searchsecurity.techtarget.com/defi nition/asymmetric-cryptography
[7] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2 (1978): 120-126.
[8] Thangavel, M., et al. "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)." *Journal of Information Security and Applications* 20 (2015): 3-10.
[9] Sharma, Sonal, Jitendra Singh Yadav, and Prashant Sharma. "Modified RSA public key cryptosystem using short range natural number algorithm." *international Journal* 2 (2012).
[10] Cryptography and Network Security Atul Kahate Tata McGraw-Hill Education, 2003 - Computer networks (pg. 76-84)