Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 8; April-June, 2015 pp. 30-33

http://www.krishisanskriti.org/acsit.html

Substitution based Encryption Decryption Technique by using DES and RSA

Davinderpreet Kaur[1] and Brahmaleen Kaur[2]

[1,2]Department of Computer Engineering Punjabi University Patiala
E-mail: [1]preetdavinder.91@gmail.com, [2]brahmaleen_sidhu@yahoo.co.in

Abstract—*Encryption play main role in information security system .Security plays very important role in communication system and internet. Internet and network growing very fast, so they need to protect the information, data and other applications are increased which can communicate over the internet. Encryption algorithms provide the secure communication over the network.*
This paper aims to a new security protocol using hybrid encryption technique for information security system to provide more efficient and secure communication .The hybrid encryption technique is combination of symmetric and asymmetric cryptographic technique. This paper comprise and provide a new hybrid method of encryption/decryption of data in blocks , based on operations of substitution and rotation operations. By combining these techniques we evaluate the performance matrices in the term of encryption and decryption time with their computational execution timings in seconds and analysis and throughput over the text size and key sizes. In this by the enhancement of new ten rounds after the encryption ,On the place of sixteen rounds of DES.

Keywords: *Asymmetric key, DES (data encryption standard), RSA (Rivest-Shamir –Adelman),Symmetric key.*

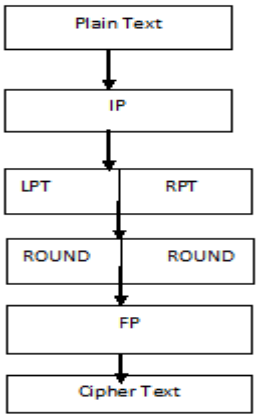
1. INTRODUCTION

There are many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Keys play an important role. If weak key is used in algorithm then everyone may decrypt the data. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user. There is no need for distributing them prior to transmission. However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power.

In this paper includes four sections Describes DES algorithm 2. Design methodology 3. Per-posed Asymmetric Algorithm 4. Results and discussions from the proposed work 5. Conclusion and future work

2. DES ALGORITHM

Actually the DES is a 16-iteation (round) cipher, with 64-bit block size. It encrypts a 64-bit input plaintext into a 64-bit output cipher-text using a 64-bit key.



The 64-bit key contains 56 independent key bits, which determine the exact cryptography transformation, and 8 bits that may be sued as parity bits for error detection after a while will see how DES dose work, as well as explain these iteration (rounds). The DES algorithm enciphers and deciphers data in 64-bit blocks under the control of a 56-bit key.

3. DESIGN METHODOLOGY

Since there is no secret key exchange required in order to use asymmetric algorithms, you might be tempted to solve the symmetric key exchange problem by simply replacing the

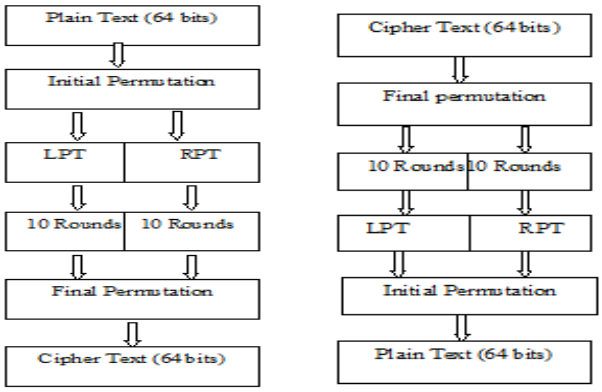
symmetric algorithm with an asymmetric algorithm. We still want to take advantage of the superior speed and security offered by symmetric algorithms, so instead, we actually combine the two (and sometimes more than two) algorithms.

The proposed asymmetric algorithm which takes the idea from symmetric algorithm and is implemented in asymmetric algorithm which will increase the security level in the data transmission communication

Generally RSA and DES both are encryption mechanism. But RSA produces the single key encryption and single key decryption. Single key encryption and decryption has high rate of predictability. So enhance this algorithm by attaching DES to it, such that security level can be increased. Each involves 10 rounds encryption and decryption which provides the extra encryption to the algorithm. Even if the encryption and decryption keys are known to others but the 10 round mechanism cannot be known and one cannot decrypt the message unless user knows the 10 rounds.

4. PROPOSED ASYMMETRIC ALGORITHM

This algorithm is based on fundamental attributes of cryptography: substitution and transposition. It consists of 10 steps, each of which is called a round. Each round performs the steps of substitution and transposition. 10 rounds of Encryption, and Decryption algorithm.



If we combine the two cryptographic mechanism, so to achieve the better of two and till extent some of the following requirements can met

- Complete secure solution
- Time taken by the encryption and decryption process is less
- Generated cipher is of compact size
- Key distribution problem is solved

5. RESULTS AND DISCUSSIONS

The advantage of asymmetric encryption is in its functionality. It provides security in a wide range of applications that cannot be solved using only symmetric techniques.

However, a price is paid for this in computational efficiency and increased cost. In many settings, the efficiency problem can be overcome by combining both algorithms, as in the following example:

- A message is encrypted with a symmetric key, which is chosen and used for this transaction only.
- This symmetric key is encrypted with the recipient's public key.
- Both the encrypted message and the encrypted key are sent to the recipient, who decrypts the symmetric key with his private key, and then uses it to decrypt the message.

This method combines the efficiency of symmetric encryption with the advantages of an asymmetric setting.

It describes and compares the two encryption methods in relation to authentication applications, and outlines the issues connected with authentication. Authentication is used in many settings that require users to prove their identity. For example, when users log in to a PC, local network or remote server, or when accessing a restricted website, their identity and access permissions must be authenticated, using symmetric and/or asymmetric authentication techniques.

RSA performance analysis of encryption algorithm Encryption key size 22bits

Decryption key size 10bits

Table 1: RSA Encryption and Decryption Methods Computational Execution Timings in Seconds

Text size	Encryption	Decryption
128 Bits	0.0548	0.0548
256Bits	0.1097	0.0548
512 Bits	0.2167	0.1648
1k	0.3856	0.3286
2k	0.7152	0.6583
5k	1.7022	1.7022
10k	3.502	3.502

DES performance Analysis of encryption algorithm key size 56 bit

Table 2: DES Encryption And Decryption Methods Computational Execution Timings in Seconds

Text	Encryption	Decryption
128 Bits	0.054845	0.00001
256Bits	0.054846	0.00001
512 Bits	0.070876	0.00053
1k	0.1417	0.0010
2k	0.2735	0.0020
5k	0.6916	0.0074
10k	1.3701	0.0132

PERFORMANCE ANALYSIS OF PERPOSED ALGORITHM

Table 3: PROPOSED ALGORITHM Encryption And Decryption Methods Computational Execution Timings in Seconds

Text size	Encryption	Decryption
128 Bits	0.109835	0.05391
256Bits	0.1664846	0.05391
512 Bits	0.280676	0.16432
1k	0.5254	0.3305
2k	0.9966	0.5513
5k	2.3747	1.7303
10k	4.7621	3.4162

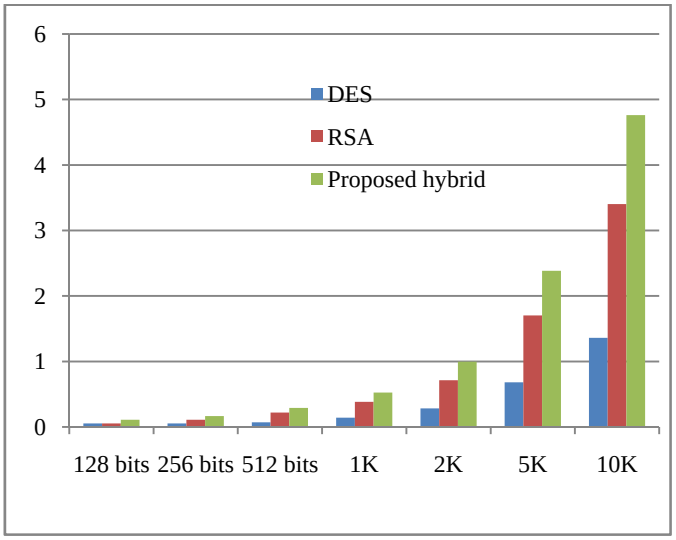


Fig. 1: encryption analysis of des, rsa, PROPOSED

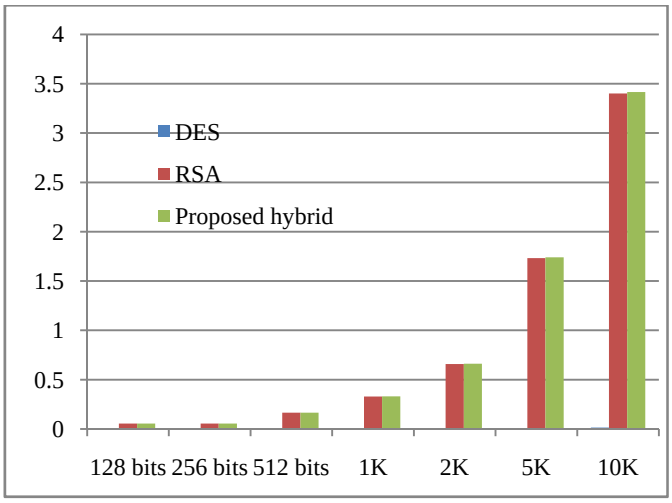


Fig. 2: DEcryption analysis of des, rsa, PROPOSED

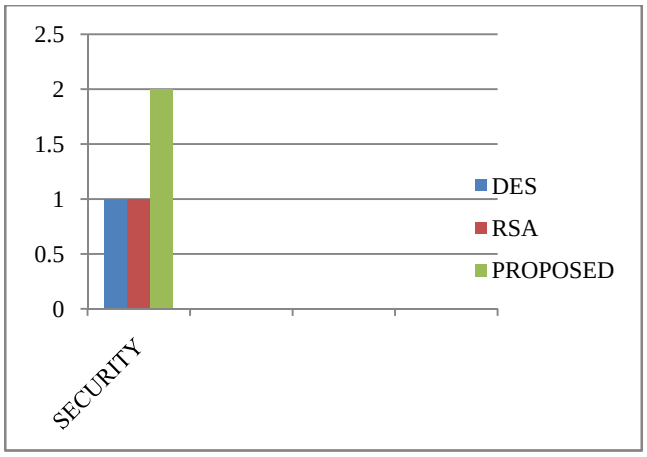


Fig. 3: SECURITY LEVEL OF DES, RSA, PROPOSED

Table 6: Summarizes the application issues discussed in this paper and their recommended encryption methods:

METHOD	des	rsa	pROPOSED hYBRID
Complexity	O(Log N)	O(N3)	O(Log N +N3)
security	modrate	high	highest

Table 5.4 Application issues governing symmetric and asymmetric techniques

Application Issue	Symmetric Encryption	Asymmetric Encryption
e-Commerce	Less secure	More secure
Ease of key management	Difficult	Easy
functionality	Difficult	Easy
High level security	less	More
Secure key transmission	Less secure	More secure
Key update	Difficult	Easy
Future growth	Less	More
Signature non repudiation	Less	Easy

6. CONCLUSIONS AND FUTURE WORK

As the performance of DES in decryption process is quiet high than other techniques. Despite the key distribution DES is more suitable to the applications which has the decryption as the highest priority, but when we talk about security there is no doubt than asymmetric key cryptography system provides more security. But by combining both the algorithms we can cover the disadvantages of both symmetric and asymmetric key cryptography to some extent.

The encryption and decryption time of the proposed algorithm can be reduced by using some ideas from the techniques like NTRU(Nth degree truncated polynomial ring unit) and this algorithm can also be used in wireless sensor node network for secure wireless data transmission.

REFERENCES

[1] Diaa Salama Abd Elminaam[1], Hatem Mohamed Abdual Kader[2], and Mohiy Mohamed Hadhoud[2] "Evaluating The Performance of Symmetric Encryption Algorithms" International Journal of Network Security, May 2010 "

[2] Ritika Chehal, Kuldeep Singh "Efficiency and Security of Data with Symmetric Encryption Algorithms, International Journal of Advanced Research in Computer Science and software Engineering, Volume 2, Issue 8, August 2012"

[3] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud "Performance Evaluation of Symmetric Encryption Algorithms, Communications of the IBIMA Volume 8, 2009 SSN: 1943-7765 "

[4] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram "International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037"

[5] Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud "Performance Evaluation of SymmetricEncryption Algorithms on Power Consumption for Wireless DevicesInternational Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009 1793-8201 "

[6] Ruangchaijatupon, P. Krishnamurthy, "*Encryption and Power Consumption in Wireless" LANs-N*, The Third IEEE Workshop on Wireless LANs – September 27-28, 2001- Newton, Massachusetts"

[7] [1]Challa Narasimham, [2]Jayaram Pradhan "EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILESJournal of Theoretical and Applied Information Technology © 2008 JATIT."

[8] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, PP. 137-139, March 2001."

[9] [1]SHAHZADI FARAH, [2]M. YOUNAS JAVED, [3]AZRA SHAMIM, [4]TABASSAM NAWAZ "An experimental study on Performance Evaluation of Asymmetric Encryption algorithms"

[10] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication, IJCST Vol. 2, Issue 2, June 2011"

[11] Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files

[12] R.L.Rivest, A.Shamir, L.Adleman "A method for obtaining digital signatures and Public-Key Cryptosystems", Communications of the ACM 21 (1978), 120-126.

[13] S.Z.S. Idrus, S.A.Aljunid, S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security,VOL.8 No.1, January 2008, PP 20-25.

[14] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005.First International Conference ,2006-02-27, PP. 84-89.

[15] D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength against Attacks." IBM Journal of Research and Development,May 1994, pp. 243 -250.