IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 2, Ser. II (Mar - Apr 2019), PP 07-10
www.iosrjournals.org

Message Security Using RSA-DES Hybrid Cryptography

Dr. Sheetalrani R. Kawale
Assistant Professor, Dept. of Comp. Sci., KSAWU, Vijayapura, Karnataka, India
Corresponding Author: Dr. Sheetalrani R Kawale

Abstract: *Cryptography is the way through which the data can be secured by encrypting and then decrypting at secured location. Encryption is the process or technique through which data can be transferred in to unreadable form. Decryption is the process or technique through which unreadable form data can be transferred in to readable form by using a key. A key either same or different is used to encrypt or decrypt data by authorized user. Based on these keys there are different types of cryptography techniques such as secret key cryptography, public key cryptography and Hash cryptography. Even now-a-days hybridization is used to merge two or more techniques to develop a new and improved form. So in our proposed paper we will try to use hybrid cryptography with RSA and DES cryptography algorithms and verify the results with other hybrid cryptography algorithms so that the data can be transferred to the destination safely.*

Key Words: *Cryptography, DES, RSA, 3-DES, Hybridization.*

Date of Submission: 26-02-2019 Date of acceptance: 12-03-2019

I. Introduction

Cryptography is the way through which the data can be secured by encrypting and then decrypting at secured location. Encryption is the process or technique through which data can be transferred in to unreadable form [2]. Decryption is the process or technique through which unreadable form data can be transferred in to readable form by using a key. A key either same or different is used to encrypt or decrypt data by authorized user. Based on these keys there are different types of cryptography techniques such as secret key cryptography, public key cryptography and Hash cryptography [5].

II. Existing System

In the existing system, there are many cryptography algorithms such as DES, RSA, AES and 3DES. Security is one of the important parameters for providing secure data transfer so one of these algorithms or a new algorithm can be used for providing security for data to be transferred and received on open network [3]. The message that has to be transmitted from source to destination node is first encrypted. The encrypted message is transferred from source to destination. At the destination node the message is decrypted to obtain the initial message[4].

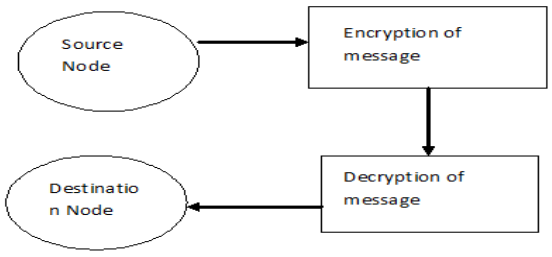

Figure 1.1: Message Transmission

III. Problem Identification

Even now-a-days hybridization is used to merge two or more techniques to develop a new and improved form. So in our proposed work we will try to use hybrid cryptography with current used cryptography algorithms and verify the results so that the data can be transferred to the destination more safely.

IV. Proposed system design description:

Hybrid encryption is the way to combine multiple encryption systems. It mainly deals with the asymmetric and symmetric methods with the strengths dealing with speed and security. There are two keys namely public and private keys which actually deal with the asymmetric and symmetric methods and the encryption is secure as long as these keys are secure. The main use of public key is that it is used to encrypt the plain test message for an encryption of the system. The user can use the key to get back the message signal after getting back the decrypted symmetric key. The main use of combination of two system is that a communication channel is established between the two users, sets of equipment through the hybrid encryption. With the continuous and indefinite use of the symmetric encryption we can enhance the process as the assymmetric encryption slows down the process .

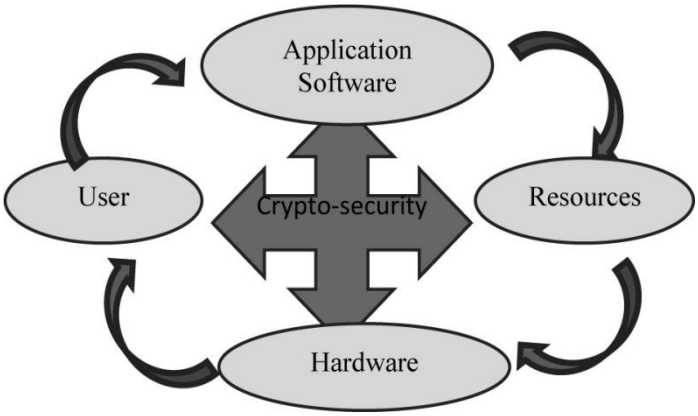

Figure 1.2: Crypto-Security

Above figure shows the security of encryption among the various sources involved like Hardware, Resources, Application Software, and mainly the User.

The process of encryption is all about the public and private keys. It starts with the obtaining of the first user public key. And then the fresh symmetric key is generated and we can encrypt the message using the newly formed key. With the use of first user public key we can encrypt the symmetric key and can send both of the encryption to first user. The message which we obtain first by the user can be called as the plain text message. The encrypted message which reaches the first user can be call as cipher text. As it is hybrid encryption it can be called as the hybrid cipher text. Next process is the decryption of the message which happens when the first user uses his personal secret key to decrypt the symmetric key and with which the first user can use symmetric key to decode the encrypted information.

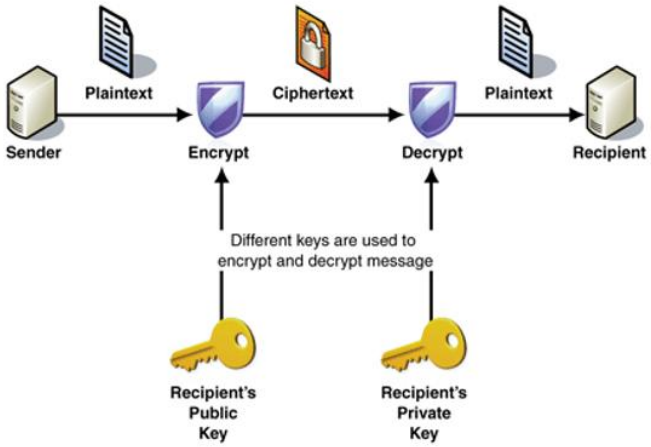

Figure 1: Asymmetric Encryption

The above diagram shows the process of encryption taking place by the use of the important keys such as the public and the secret keys and the decryption of the message signal.

4.1. RSA-DES HYBRID CRYPTOGRAPHY ENCRYPTION ALGORITHM:

RSA (Rivest, Shamir and Adleman) is an asymmetric cryptography algorithm that uses two keys public key and private key for encryption and decryption where as DES ((Data Encryption Standard) is a asymmetric cryptography algorithm which uses only one key for encryption and decryption. These two cryptography algorithms are combined together and modified, hybridized form is implemented. RAS is used to perform key encryption and DES is used for data encryption. This results in faster execution and the user is free to use a number of encryption keys for their transfer of data in maximum secured manner.

V. Conclusion

Hybrid cryptography is used for providing better message security. We combined asymmetric algorithm i.e. RSA and symmetric algorithm DES for message encryption. We have compared various approaches and found combination of DES and RSA to be most efficient. Our approach mainly compared the key generation and ciphering time. We can determine the efficiency of different hybrid algorithms based on time and memory consumption.

Table 1: Hybrid of AES, DES &3DES with RSA Comparison

	RSA-AES		RSA-3DES		RSA-DES	
Text Size (bits)	Time Taken (ms)	Memory Consumed (Kb)	Time Taken (ms)	Memory Consumed (Kb)	Time Taken (ms)	Memory Consumed (Kb)
512	303	54840	301	47645	269	37614
256	295	52460	275	36528	252	33580
56	264	32550	205	31465	273	35589

RSA-AES:
Time taken = 264ms
Encrypts and Decrypts 56bits of text data
Consumes 32550kb of memory
RSA-DES:
Time taken = 205ms
Encrypts and Decrypts 56 bits of text data
Consumes 31465kb of memory
RSA3-DES:
Time taken = 273ms
Encrypts and Decrypts 56 bits of text data
Consumes 35589kb of memory

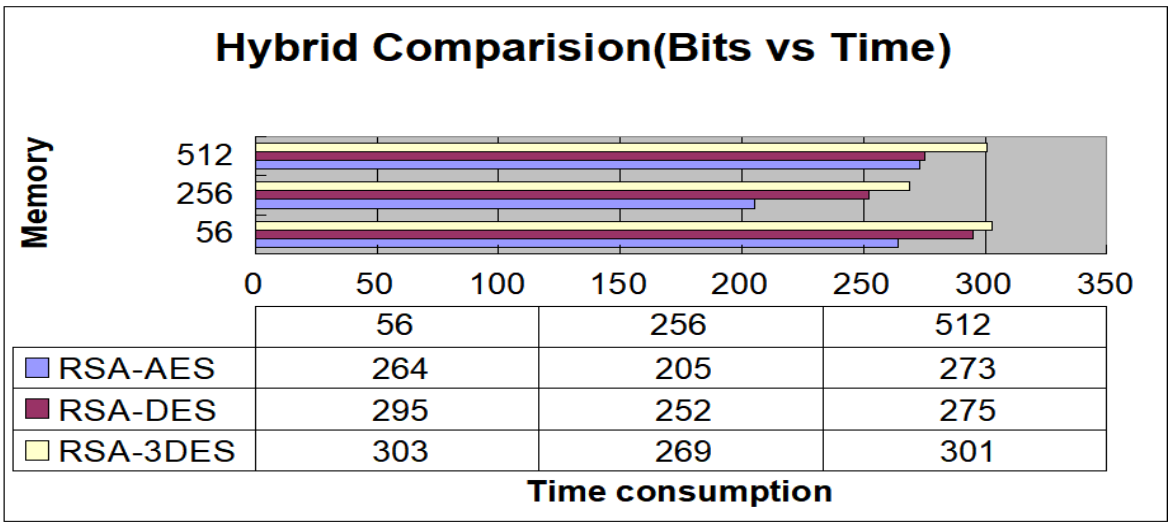

Figure 1.4: Hybrids Time vs. Bits Comparison

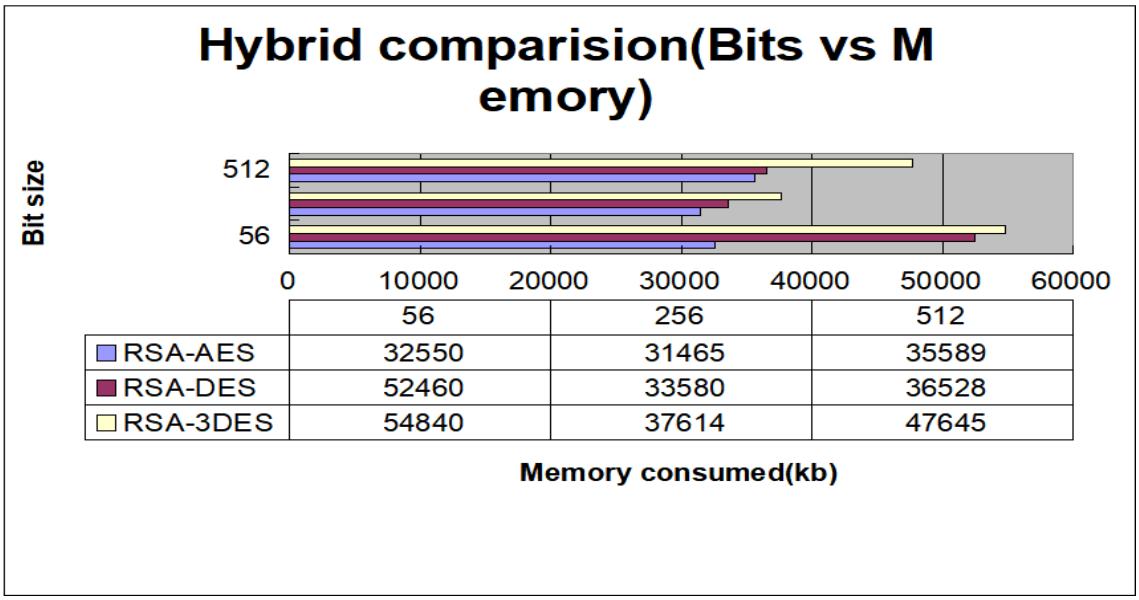

Figure 1.5: Hybrids Memory vs. Bits Comparison

By looking at the comparisons between the proposed hybrid algorithm (shown in table 1) we can say that RSA-DES is the most efficient algorithm among all the respective hybrid techniques.

Acknowledgement

I would like to acknowledge my guide Dr. Ramesh K. for guiding me and for his kind support.

References

[1]. J Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah, C.N., Ganjali, Y. and Diot, C. "Characterization of failures in an operational IP backbone network", IEEE/ACM Transactions on Networking (TON), 16(4), pp.749-762. 2008

[2]. Van Tilborg, H.C. and Jajodia, S. eds." Encyclopedia of cryptography and security", Springer Science & Business Media, 2014

[3]. Armknecht, F., Iwata, T., Nyberg, K. and Preneel, B. "Symmetric Cryptography", [Dagstuhl Seminar 16021] In Dagstuhl Reports (Vol. 6, No. 1). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016

[4]. Sousa, L., Antao, S., Kelley, K., Jiang, N., Harris, D.M. and Pinckney, N. *Public Key Cryptography. In Circuits and Systems for Security and Privacy* (pp. 133-206). CRC Pres, 2016.

[5]. Emmett, J., Eisen, P.A., Muir, J. and Murdock, D., Irdeto BV, 2016." Method and system for protecting execution of cryptographic hash functions", U.S. Patent 9,443,091.

[6]. T. He, P. Vicaire, T. Yan, L. Luo, L. Gu, G. Zhou, R. Stroleru, Q. Co, J. Stankovic, and T. Abdelzaher, Real-Time Analysis of Tracking Performance in Wireless Sensor Networks, IEE Applications Real-Time Symposium, May 2006.

[7]. Sheetalrani R Kawale, Aziz Makandar "Incorporating Concepts of Nanotechonology Services and Computing For Smart Classrooms" Research Paper Research Link – 100, Vol –XI (5), Page No. 26-29 RNI No. MPHIN- 2002-7041, ISSN No.-0973-1628, July 2012.

[8]. Sheetalrani R Kawale, Aziz Makandar " Enhancing Energy Efficiency in WSN using Potential Concepts" International conference on Advances in Computer and Electrical Engineering (ICACEE'2012), 2012 manila (Philippines) ISBN: 978-93-82242-11-6 Page No. 118-122, Nov. 17-18.

[9]. Sheetalrani R Kawale, Aziz Makandar, Ramesh K "Enhancing Energy Efficiency in WSN using Energy Potential And Energy Balancing Concepts" International Journal of Innovative Research in Information Security (IJIRIS) volume 1, Issue 2, ISSA*/2349-7009(Online) ISSN /2349-7017 (Print) Page no. 15-17, August 2014

[10]. Sheetalrani R Kawale, Shruti P "RECR Routing Algorithm In Wireless Sensor Network" International journal Of Emerging Technology & Research(IJETR) Volume 1, Issue 6, ISSN(E):2347-5900 ISSN (P):2347-6079 Page no. 89-91, Sep-Oct, 2014.

BIOGRAPHY

Dr. Sheetalrani R. kawale is serving as an Assistant Professor in the Department of Computer Science at the Karnataka State Akkamahadevi Women's University, Vijayapura. She has 14 yrs of teaching experience and pursued PhD in the Computer Science field. Her area of interest is in Networking.

Dr. Sheetalrani R Kawale. " Message Security Using Rsa-Des Hybrid Cryptography " IOSR Journal of Computer Engineering (IOSR-JCE) 21.2 (2019): 07-10.