Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Literature Review of Various Variants of RSA Cryptosystem

Mr. Gagendra Singh Chandel*
HOD,SSSIST Sehore
India

Prabhat Kumar Singh
M.Tech Scholar,SSSIST Sehore
India

***Abstract*— This research paper concentrates on the different kinds of encryption techniques that are existing. It is a literature survey of some modern cryptography techniques. The advantages and disadvantages of the methods are also discussed in brief. It also aims image encryption techniques, double encryption, information encryption techniques and Chaos-based encryption techniques.**

***Keywords*— RSA,Private Key,Public Key,Encryption,Decryption,** *Weiners attack.*

I. INTRODUCTION

In this age of universal electronic connectivity of viruses and hackers of electronic eavesdropping and electronic fraud. There is indeed needed to store the information securely. This led to a heightened awareness to protect data and resources from disclosure to guarantee the authenticity of data and messages, and to protect systems from network-based attacks[1] . Cryptography the science of encryption. It plays a central role in mobile phone communications, e-commerce, sending private emails, sending financial information, safety of ATM cards, computer access passwords, for electronic commerce digital signature and touches on many aspects of our daily lives . Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message plaintext into one that is unintelligible cipher text and then retransforming that message back to its original form .In modern times, the cryptography is considered to be a branch of both mathematics and computer science, and it is affiliated closely with information theory and engineering. Although in the past cryptography referred only to the encryption and decryption of message using secret keys. The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted/scrambled by any encryption algorithm using the 'key'. Only the user having the access to the same 'key' can decrypt/de-scramble the encrypted data. This method is known as private key or symmetric key cryptography. There are several standard symmetric key algorithms defined. Examples are AES, 3DES etc. These standard symmetric algorithms defined are proven to be highly secured and time tested. But the problem with these algorithms is the key exchange. The communicating parties require a shared secret, 'key', to be exchanged between them to have a secured communication. The security of the symmetric key algorithm depends on the secrecy of the key. Keys are typically hundreds of bits in length, depending on the algorithm used. Since there may be number of intermediate points between the communicating parties through which the data passes, these keys cannot exchange online in a secured manner. In a large network, where there are hundreds of system connected, offline key exchange seems too difficult and even unrealistic. This is where public key cryptography comes to help. Using public key algorithm a shared secret can be established online between communicating parties without the need for exchanging any secret data.

II Objectives

There are so many algorithms present to encrypt and decrypt the data for security purpose in cryptography. RSA is the most common algorithm for encryption and decryption. But still the current versions are slow and less secure. The objective of the proposed algorithm is to propose a faster variant of RSA algorithm & also make it more secure against Weiners attack.

III Literature Survey

Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul. Elminaam et.al., (2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results. First; in the case of changing packet size with and with out transmission of data using different architectures and different WLANs protocols, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. DES and 3DES are known to have worm holes in their security mechanism, Blowfish and AES do not have any so far[6]. Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files designed by challa Narasimham and Jayaram Pradhan(2008)- They performed the performance comparison for variable sized text files as input. An analysis on computational running times results in significant difference among the methods. He believe in that the performance of DES, especially in decryption method is very high than the alternatives. Despite the key distribution, DES is more suitable to the application, which has the decryption as the highest priority.He has proposed and performed the test cases on the two PKCS methods i.e., RSA and NTRU Though the encryption, decryption and complexity are high in NTRU,

the RSA provides the highest security to the business application. He presented all these parameters with computational running times for all the methods, so as to select the appropriate method[7].

Abdel-Karim and his colleague Al Tamimi presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power.

P. Prasithsangaree and his colleague P. Krishnamurthy have analyzed the Energy Consumption of RC4 and AES Algorithms in Wireless LANs in the year 2003.They have evaluated the performance of RC4 and AES encryption algorithms. The performance metrics were encryption throughput, CPU work load, energy cost and key size variation. Experiments show that the RC4 is fast and energy efficient for encrypting large packets. However, AES was more efficient than RC4 for a smaller packet size. From the results, it appears that we can save energy by using a combination of RC4 and AES to provide encryption for any packet size. The tradeoffs with security are not completely clear[9]. Comparative Analysis of AES and RC4 Algorithms for Better Utilization has designed by Nidhi Singhal, J.P.S.Raina in the year (2011).The performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments show that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of the research, RC4 is better than AES.we compare the encryption time of AES and RC4 algorithm over different packet size. RC4 takes less time to encrypt files w.r.t. AES. In AES, CFB and CBC takes nearly similar time but ECB takes less time then both of these[10]. Efficiency and Security of Some Image Encryption Algorithms Marwa Abd El-Wahed et.al (2008) – worked in this paper, four image encryption algorithms have been studied by means of measuring the encryption quality, the memory requirement, and the execution time of the encryption. In addition, the security analysis of these schemes is investigated from cryptographic viewpoint; statistical and differential attacks. The results are compared, focusing on those portions where each scheme is performed differently A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms *designed by* S.A.M Rizvi1 et.al., All algorithms run faster on Windows XP. The CAST runs slower than AES for text. Blowfish encrypts images most efficiently on all 3 platforms, even CAST runs faster on Windows XP for image data. But on Windows Vista and Windows7, AES and CAST perform at the similar speed .CAST performs better than BLOWFISH and AES on Windows XP for encrypting audio files, but on Windows Vista and Windows7, there is no significant difference in performance of

CAST and AES, however BLOWFISH encrypts audio files at less speed for audio files[12]. ThroughPut Analysis of Various Encryption Algorithms presented by Gurjeevan Singh et al.,(2011)- For experiment a Laptop with 2.20 GHz C.P.U., 4GB RAM Core-2-Dou Processor and Windows 7 Home Premium (32-Bit) is used in which the performance data are collected. In this experiment software encrypts the text file size that ranges from 20 Kb to 99000 Kb. Their implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm.The performance matrices are throughput. The throughput of encryption as well as decryption schemes is calculated but one by one. In the case of Encryption scheme throughput is calculated as the average of total plain text in k bytes divided by the average Encryption time and in the case of Decryption scheme throughput is calculated as the average of total cipher text is divided by the average Decryption time. This work presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. The presented simulation results show the numerous points. Firstly it was concluded that Blowfish has better performance than other algorithms followed by AES in terms of throughput. Secondly 3DES has least efficient of all the studied algorithms[15].

IV. Problem Definition

There are so many algorithms present to encrypt and decrypt the data for security purpose in cryptography. RSA is the most common algorithm for encryption and decryption. But still the current versions are slow and less secure. The objective of the proposed algorithm is to propose a faster variant of RSA algorithm & also make it more secure against Weiners attack.

V. Conclusion

In this paper the existing encryption techniques are studied and analyzed. All the techniques are useful for real-time encryption. There advantages and disadvantages are discussed. It is found that a faster version of RSA may be proposed. Also there is a need to remove wieners and some other similar attacks.

References

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
[2] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.
[3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[4] Ramesh G, Umarani. R, " Data Security In Local Area Network Based On Fast Encryption Algorithm", International Journal of Computing Communication and Information System(JCCIS) Journal Page 85-90. 2010.
[5] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.
[6] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[7] Challa Narasimham, Jayaram Pradhan," EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILES" Journal of Theoretical and Applied Information Technology,pp55-59 2008.

[8] Abdel-Karim Al Tamimi," Performance Analysis of Data Encryption Algorithms "

[9] Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

[10] Nidhi Singhal1, J.P.S.Raina2, Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011 pp177-181.

[11] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry," Efficiency and Security of Some Image Encryption Algorithms", Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[12] Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa" A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms",

[13] Turki Al-Somani ,Khalid Al-Zamil "Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems", Theses

[14] 1Gurjeevan Singh, 2Ashwani Kumar Singla, 3K.S. Sandha," Through Put Analysis of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011

[15] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.

