RESEARCH ARTICLE OPEN ACCESS

A Modified Technique For Performing Data Encryption & Data Decryption

Prabhat Kumar Singh[1], Gajendra Singh Chandel[2]

M. Tech Scholar, SSSIST, Sehore, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal(MP), India.[1]

HOD CSE, SSSIST, Sehore, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal(MP), India.[2]

Abstract
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, in turn, 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. Information security via encryption decryption techniques is a very popular research area for many people's over the years. This paper elaborates the basic concept of the cryptography, specially public and private cryptography. It also contains a review of some popular encryption decryption algorithms. A modified method is also proposed. This method is fast in comparison to the existing methods.

Keywords-AES, DES, Decryption, Encryption, RSA

I. Introduction

Cryptography the science of encryption, plays a central role in mobile phone communications, pay-tv, e-commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, 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, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Although in the past cryptography referred only to the encryption and decryption of message using secret keys. Nowadays, cryptography generally classified into two categories, the symmetric and asymmetric. The RSA algorithm is a Asymmetric/Public key cryptography for encryption and decryption.

II. Related Work

Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul. El minaam 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 without 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 collegeue 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 eencryption 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].

Common Problems in Existing RSA Variants:

- The main disadvantage of RSA encryption its slower speed
- Not secure against wiener's attack
- Problem arise to common modulus attack
- known plaintext attack are possible
- Low decryption exponent attack if we know the decryption exponent.
- The decryption time slow.

III. Proposed Approach

The steps of the proposed work are as follows:

1. First choose random large prime integers p and q of roughly the same size but not too close to each other.
2. Calculate the product n = pq (ordinary integer multiplication)
3. Choose a random encryption exponent e It must not has any common factor with either p-1 or q-1.
4. Compute ed mod (p-1) * (q-1) = 1
5. Encryption Step:
   $c = m^e \bmod n$
6. Decryption Step:

In this step, we will use the larger value of d. Also we will split the n in to p and q. Then we will compute the plain text by applying the Fermat's theorem as follows:

- First compute
  $X1 = c^{dp} \bmod p$
  $X2 = c^{dq} \bmod q$
  Where $dp = d \bmod p-1$
  &
  $dq = d \bmod q-1$

- The compute
  W = (X2 – X1) * W1 mod q
  Where W1 = p modinverse q
- Then finally compute
  M= c^d mod n = X1 + W * p

IV. EXPERIMENTAL RESULT

We implemented the existing version of RSA & the proposed variant in Java. The summary of their performance comparison is as follows:
Plain Text Used For Experimental Study:

Input 1

12131415161718191213141516171819121314
12131415161718191213141516171819121314

12131415161718191213141516171819121314

12131415161718191213141516171819121314

12131415161718191213141516171819121314

12131415161718191213141516171819121314

Table 1: Performance Comparison

Method	Decryption Time
RSA Existing Variant	29ms
Proposed RSA Variant	21ms

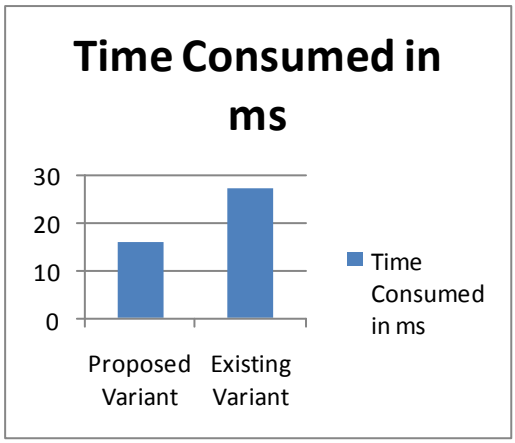

Figure 1: Proposed Variant v/s Existing Variant

Input 2;

We tested the code with one more input:
567567678678789898989
787856346377347364734
335673265358356326538
336473267327856322657

Table 2: Performance Comparison

Method	Decryption Time
RSA Existing Variant	19ms
Proposed RSA Variant	14ms

V. Conclusion

In this paper, we have elaborated the basic concept of cryptography and the key management schemes. A review of modern methods is also done in brief. A modified method for performing the encryption and decryption is also proposed. The encryption of our proposed cryptosystem is faster in comparison to current variants of RSA cryptosystem. Also our proposed cryptosystem is more secure against low decryption exponentiation attack, because we are using a large value of d. Also decryption time will be less in comparison to the existing method.

References

[1] Dr.Alaa Hussein Al-Hamami, Ibrahem Abdallah Aldariseh, "*Enhanced Method for RSA Cryptosystem Algorithm*" International Conference on Advanced Computer Science Applications & Technologies, 2012 PP 402-408

[2] Atul Kahate ―*Cryptography and Network Security 3rd edition.*

[3] William Stallings " *Network Security Essentials (Applications and Standards)*", Pearson Education, 2004 .PP268-275

[4] 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

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

[6] 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.

[7] 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.

[8] Dr. S.A.M Rizvi1, Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa" *A Comparative StudyOf Two Symmetric*

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

Prabhat Singh, BE in Computer Science and Engineering and Pursuing M.Tech in Information Technology from SSSITS, Sehore, (M.P).India . He has published six research papers in reputed journals. His research interests are in Cloud Computing and network Security.

Gajendra Singh Chandel is working in SSSITS Sehore, M.P. India as HOD in Computer Science and Engineering Department. He has Guided more than 50 M.Tech Scholars.