ISSN 22773061

Comparative Study of DES, 3DES, AES and RSA

Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh

Abstract

In today world importance of exchange of data over internet and other media type is eminent; the search for best data protection against security attacks and a method to timely deliver the data without much delay is the matter of discussion among security related communities. Cryptography is one such method that provides the security mechanism in timely driven fashion. Cryptography is usually referred to as "the study of secret", which is most attached to the definition of encryption. The two main characteristics that identify and differentiate encryption algorithm from another are their capability to secure the protected data against attacks and their speed and effectiveness in securing the data. This paper provides a comparative study between four such widely used encryption algorithms DES, of DES, 3DES, AES and RSA on the basis of their ability to secure and protect data against attacks and speed of encryption and decryption.

Keywords: Encryption Algorithm, Performance, AES, DES, 3DES, RSA, Cryptography.

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 9, No 3

editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 22773061

Introduction

As we know that demand of internet is increasing day by day as to transfer data or other media types on the internet. Now it's the responsibility of the service provider to provide necessary security against the data thieves' attacks and providing the service under timely manner. In this paper, we have compared the most commonly used algorithms for data encryption. Our main concern in this paper is to determine the performance of different algorithms under different settings and when different data loads are used.

We have given a quick overview of cryptography techniques and discussed the different algorithms. We have elaborated the performance evaluation methodology and settings for a better comparison.

2. Cryptography: Overview

Cryptography means "Hidden Secrets", now-a-day concerned with encryption. Cryptography is the study of techniques for secure communication. Cryptography is used for analyzing protocols, which are related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation.

2.1 Cryptography Goals

We have discussed the goals behind using cryptography. They are as follow:

Authentication: It means that the data sender and data receiver must be authenticated before sending and receiving data.

Confidentiality: It means that the user who is authenticates, can only access the messages or data of other authenticated users.

Integrity: It means that the data is free from any kind of modification between sender and receiver.

Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Service Reliability: Secure systems can be attacked by intruders, which may affect the service that is provided to the user.

2.2 Symmetric and Asymmetric encryptions

There are commonly two types of techniques that are used for encrypt/decrypt the secured data i.e. Asymmetric and Symmetric encryption techniques.

2.2.1 Symmetric Encryption

In case of Symmetric Encryption, same cryptography keys are used for encryption of plaintext and decryption of cipher text [2]. Symmetric key encryption is simpler and faster but their main drawback is that both the users need to transfer their keys in a secure way.

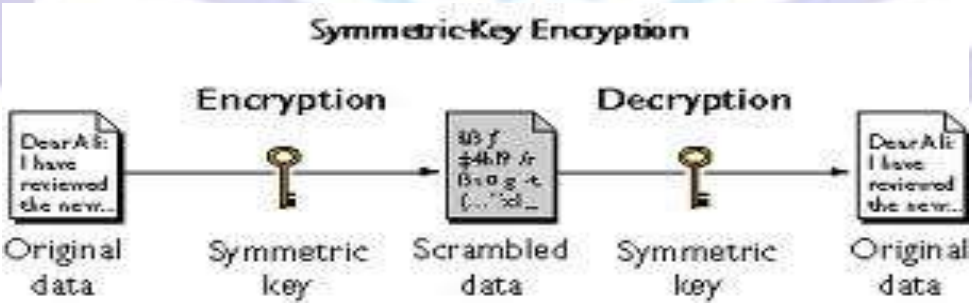


Fig. 2.1

As shown in the figure 2.1, there is only one key used both for encryption and decryption of data. So the main problem over this system is, users have to transfer their keys in a very safe manner. If the key is disclosed, then system will be collapsed.

ISSN 22773061

2.2.1 Asymmetric Encryption

In case of Asymmetric encryption, two keys are used. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is known to public and a private key which is only known to user.

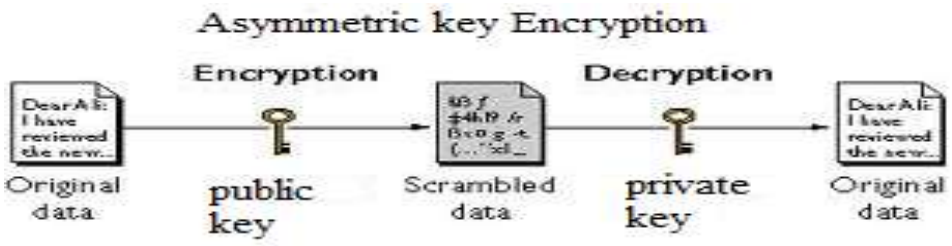


Fig. 2.2

In Asymmetric key Encryption, there are different keys that are used for encryption and decryption of data i.e. Public key and Private key.

COMPARISON OF ALGORITHMS

DES

Data Encryption Standard is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non- linear substitutions (S-boxes) and exclusive OR operations. It encrypts the data in block size of 64bits each. Same algorithm and key are used for encryption and decryption. Key is 56 bits long. The position of 8, 16,24,32,40,48,56,64 are discarded [6]. DES is based on two fundamental attributes of cryptography Diffusion (Substitution) and Confusion (Permutation) consisting of 16 rounds [10]. In each round key and data bits are shifted, permuted, XORed andsent through, 8 s-box. In the first round 64 bit plaintext is handed to initial permutation(IP).Then IP generates two halves left plaintext(LPT)and right plaintext(RPT).Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are rejoined. Decryption is same process perform rounds in reverse order.

Algorithm

[1] DES takes an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and generates output of 64 bit block.

[2] The plaintext block is subject to an shift the bits around.

[3] The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.

[4] The plaintext and key are processed in 16 rounds

Consisting of:

a. The key is split into two 28 bit halves

b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.

c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed key is used to encrypt this round's plaintext block.

d. The rotated key halves from step 2 are used in next round.

e. The data block is split into two 32-bit halves.

f. One half is subject to an Expansion Permutation to increase its size to 48 bits.

g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.

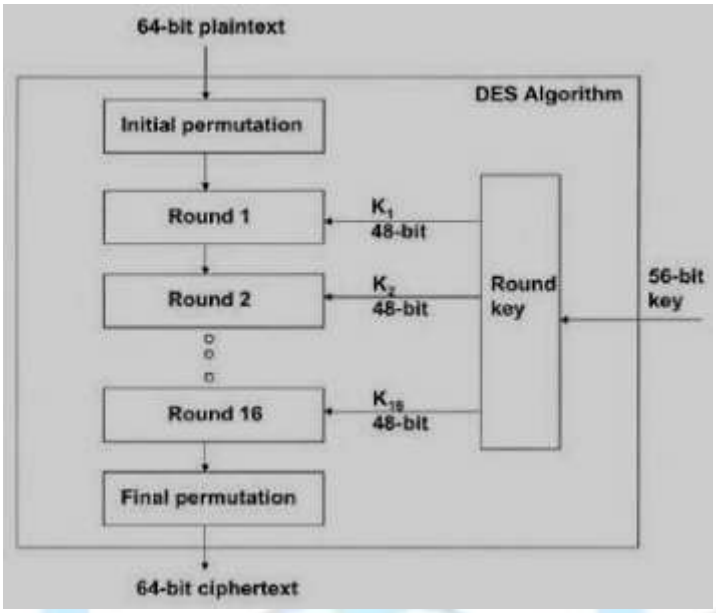
h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

i. Output of step 8 is subject to a P-box to permute the bits.

j. The output from the P-box is exclusive- OR'ed with other half of the data block.

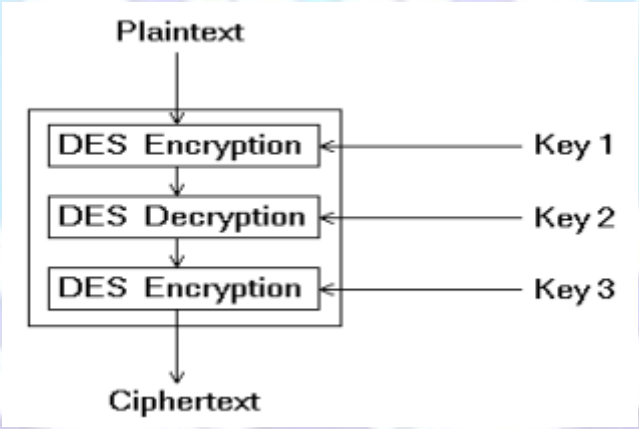
k. The two data halves are swapped and become the next round's input.

ISSN 22773061



Triple DES

As an enhancement of DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level [8]. It was used to remove the meet-in-the-middle attack occurred in 2-DES and the brute force attacks in DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.



RSA

This is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular and asymmetric key cryptographic algorithm. It may used to provide both secrecy and digital signature [2]. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0and n1 for some n values. Size of n is considered 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key.

Algorithm

Choose large prime numbers p and q such that p~=q.

Compute n=p*q

Compute φ (pq) = (p-1)*(q-1)

Choose the public key e such that gcd (φ (n), e) =1; 1<e< φ (n)

Select the private key d such that d*e mod φ (n) =1

So in RSA algorithm encryption and decryption are performed as-

Encryption Calculate cipher text C from plaintext message M such that

C=M ê mod n

Decryption

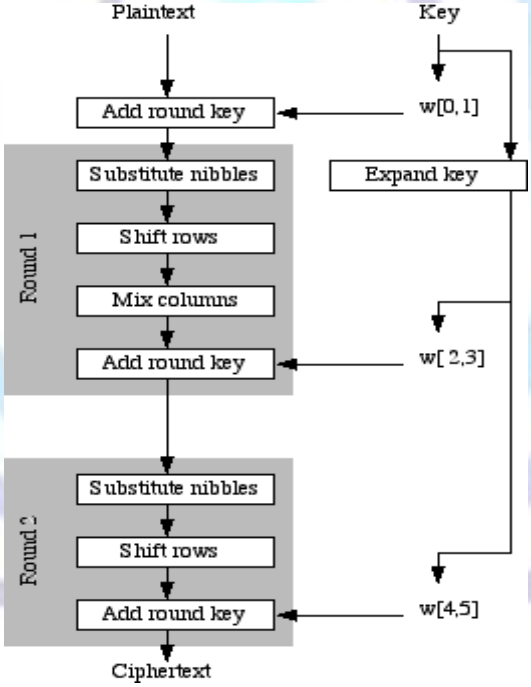
M=C^d mod n=Mêd mod n

AES

The Advanced Encryption Standard is the United State Government standard for symmetric encryption. AES is a block cipher that encrypts a 128-bit block (plaintext) to a 128-bit block (ciphertext), or decrypts a 128-bit block (ciphertext) to a 128-bit block (plaintext).AES uses a key (cipher key) whose length can be 128, 192, or 256 bits. Hereafter encryption/decryption with a cipher key of 128, 192, or 256 bits is denoted AES- 128, AES192, AES-256, respectively. AES-128, AES-192, AES-256 process the data block in, respectively, 10, 12, or 14 iterations of a pre-defined sequence of transformations, which are also called “rounds” (AES rounds) for short.

The rounds are identical except for the last one, which slightly differs from the others (by skipping one of the transformations) [6]. The rounds operate on two 128-bit inputs: “State” and “Round key”. Each round from 1 to 10/12/14 uses a different Round key. The 10/12/14 round keys are derived from the cipher key by the “Key Expansion” Algorithm. This algorithm is independent of the processed data, and can be carried out independently of the encryption/decryption phase.

The data block is processed serially as follows: initially, the input data block is XOR-ed with the first 128 bits of the cipher key to generate the “State”. This step is also referred to as “Round 0” which is using round key #0 (round key #0 is the first 128 bits of the cipher key). Subsequently, the State is serially passed through 10/12/14 rounds where the result of the last round is the encrypted (decrypted) block.



Comparative Analysis

In this paper, the popular algorithms including DES, 3DES, AES (Rijndael), RSA, were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in VB.NET, using their standard specifications, and were tested using the following parameters.

Input data size- Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of input data size, number of rounds etc. The algorithm is considered best which use small memory and perform best task.

Time- The time required by algorithm to complete the operation depends on processor speed, algorithm complexity. Less the time algorithm takes to complete its operation better it is.

Throughput-Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm.

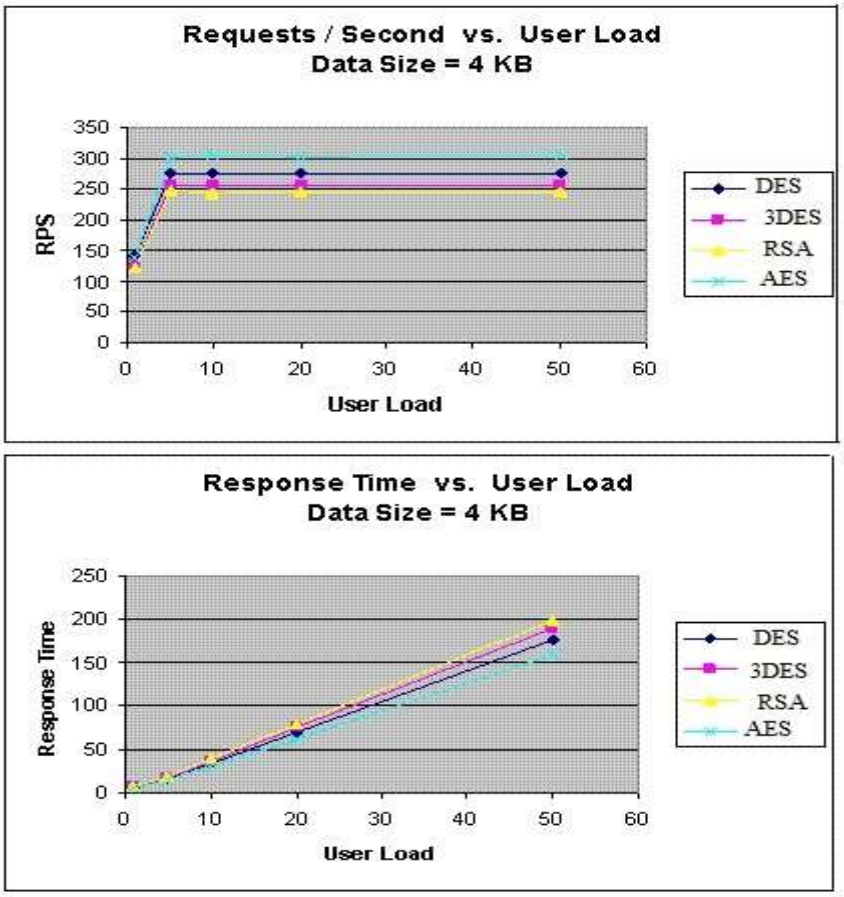


Fig. 6 Comparison results using .NET implementations

The comparison was performed on the following algorithms: DES, Triple DES (3DES), RSA and AES (Rijndael). The results shows that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.

Conclusion

Our results revealed that AES is the better algorithm in terms of performance and security although its power consumption is on higher side but it is way less than RSA and Triple DES only DES has less power consumption than AES but on security front DES is the most vulnerable and can be easily broken by brute force attack in merely fifteen hours. In comparison to RSA strength of a 128-bit AES key is roughly equivalent to 2600-bits RSA key making this the best among the compared algorithms.

References

1. Ferguson, N.,Schnier, B. and KonhoT. (2010), “Cryptography Engineering: Design principles and Practical applications”

2. Aman Kumar,Dr.Sudesh Jakhar,Mr. Sunil Maakar “Distinction between Secret key and Public key Cryptography with existing Glitches” IJEIM- 0067, vol.1, 2012.

3. Yogesh Kumar, Rajiv Munjal, “Comparison of symmetric and asymmetric cryptography with existing vulnerabilities” IJCMS-Oct.2011.

4. Atul Kahte “Cryptography and Network Security”,2nd Ed”.

5. Eli Biham and Adli Shamir, ”Differential Cryptanalysis of full DES”.

6. Dan Boneh and Glenn Durfee “Cryptanalysis of low exponent RSA”

7. W. Diffie,M.E Hellman” New Directions in Cryptography”.

8. Piper,F “Encryption”. Security and Detection, Ecos 97. European Conference

9. Schweighofer E (1997) Downloading information Info I & Common Technology.

10. Himani Agarwal &Manish Sharma” Implementation and analysis of various Cryptography” Dec-2010

11. Kofahi, N.A., Turki Al-Somani,Khalid Al- Zamil “Performance evaluation of three Encryption/ decryption algorithms”

12. Shasi Mehlrotra Seth, Rajan Mishra “ Comparative Analysis of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, June 2011

Author’ biography with Photo

Amritpal Singh received the **B.Tech.** degree in Information Technology from the Beant College of Engineering and

Technology, Gurdaspur, Punjab Technical University Jalandhar, India, in 2010. Currently pursuing **M.Tech.** in Computer Science engineering (cloud computing) in Punjab Technical University, Jalandhar, India. My research interest includes Cloud Computing, Database Management System and Network security

Mohit Marwaha received the **B.Tech.** degree in Information Technology from the Beant College of Engineering and Technology, Gurdaspur, Punjab Technical University, Jalandhar, India, in 2008. **M.Tech.** in Computer Science engineering (cloud computing) in Punjab Technical University, Jalandhar, India. My research interest includes Cloud Computing, Distributed computing and Network security

Baljinder Singh received the **B.Tech.** degree in Information Technology from the Beant College of Engineering and Technology, Gurdaspur, Punjab Technical University, Jalandhar, India, in 2008. Currently pursuing **M.Tech.** in Computer Science engineering (Network Security) in Punjab Technical University, Jalandhar, India. My research interest includes Mobile Adhoc Network and Network security

SandeepSingh received the **B.Tech.** degree in Information Technology from the Sant Baba Bhag Singh Institute of Engineering & Technology , Punjab Technical University, Jalandhar, India, in 2012. Currently pursuing **M.Tech.** in Computer Science engineering from Punjab Technical University, Jalandhar, India.