



Study and Analysis of Popular Cryptographic Algorithms

¹Pramod Singh

Research Scholar M.G.C.G.V. Chitrakoot, Madhya Pradesh, INDIA

²Dr. Bharat Mishra

Associate Professor M.G.C.G.V. Chitrakoot, Madhya Pradesh, INDIA

³Dr. P.K. Rai

Professor APS University, Rewa, Madhya Pradesh, INDIA

Abstract: In recent years database security has become an important issue for distributed environment. Encryption has come up as a solution, and plays an important role in security of distributed database. Many techniques have been developing by different organization to protect the shared data. This paper present a brief focus on cryptography to secure the data stored in database and shared in distributed environment. Firstly the data which can be stored into database must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper we setup an experimental analysis between popular encryption algorithms like AES,DES ,RSA,PGP,RC4 and RC6, with respect to CPU utilization, Memory Utilization and encryption time taken by algorithms to encrypt different size of different type files in Three layer distributed environment.

I. Introduction

Within the past decade the internet technology and database industries have revolutionized the way to people interact and shares the information. This rapid growth of technologies is creating large opportunities for developing large-scale distributed applications. These systems are made up of several interacting components which shares sensitive information. However, this phenomenal growth has also brought about security concerns. Encryption has become as a solution, and plays an important role in security of information stored and shared in distributed computing environment. The process to convert ordinary information or the plain text into unintelligible text or the cipher text in cryptography is called encryption. The cipher text is understandable only to someone who knows how to decrypt it. The message or information is encrypted using an encryption algorithm. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm which usually requires a secret decryption key.

II. Types of Encryption scheme

Many encryption algorithms are widely available for database and information security. Encryption scheme can be divided into two groups:

1. Symmetric-key

In this scheme same key is used for encryption and decryption it is also known as the secret key encryption

2. Asymmetric key

In this scheme different keys are used for encryption and decryption it is also known as the public-key encryption.

III. Comparisons of popular encryption scheme

1. DES

DES is a block cipher it uses data in blocks of size 64 bits each. 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The key length is 64 bits [1, 3,6].

2. AES

AES is also a block cipher algorithm which is based on a design principle known as a substitution-permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits [1, 2, 5].

3. RC4

RC4 is recognized as the most commonly utilized stream cipher in the world of cryptography it requiring a secure exchange of shared key [1, 7].

4. RSA

RSA is a most popular and proven asymmetric cryptography algorithm. It is based on the mathematical fact that is easy to find the private and public keys based on the very large prime numbers. [1, 2, 7].

5. RC6

RC6 is also an asymmetric key algorithm it uses 128 bits plain text with 20 rounds and a variable key length of 128 to 256 bit [1, 4, 5].

6. PGP

PGP can be used either symmetric or asymmetric form. It is fast and good for small message encryption.

Table 1: Different Encryption Algorithms

Scheme	Algorithm Type	Block Size	Key Length	Rounds	Speed	Security
AES	Symmetric Block	128 bits	128,192, 256	10 or 12 or 14	Fast	Excellent security
DES	Symmetric Block	64 bits	56-bits	16	Slow	Not strong enough
RSA	Asymmetric	Minimum 512 bits	1024	1	Slow	Excellent security
RC4	Symmetric Stream	variable	40-128-bits	256	Fast	Fast in SSL
RC6	Asymmetric	128 bits	128,192,256	20	Fast	Good security
PGP	Asymmetric and Symmetric	1	2048	1	Fast	Strong Security for Small Data

Table-1 shows a comparative summary between AES, DES, PGP, RC4, RC6, and RSA, in to four factors which are Algorithms type, Key Length, Rounds and Block Size. The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits. The key size of AES algorithm is 128, 192, 256 bits.

IV. Comparative Analysis of Selected Encryption Schemes

To select a best encryption algorithm we have conducted an experimental setup by using asp.net and SQL Server 2008. In this experiment we have design a three layer client server environment to test the performance of these algorithms with respect to Encryption Time, CPU Utilization and Memory Utilization ratio. We have taken video data in different size to check the performance because the video data has high resolutions. Table 2; shows the encryption time taken by different algorithms for different file sizes and figure1 shows that the comparative analysis of encryption time taken by different encryption algorithms.

Table 2: Encryption time taken by different algorithm

File Size In kb	Encryption time In ms					
	AES	RSA	PGP	RC4	RC6	DES
3000	20	32	29	20	26	13
5000	39	40	37	24	32	22
7000	54	56	51	35	52	34
9000	67	75	64	45	60	43
11180	76	84	76	54	71	53

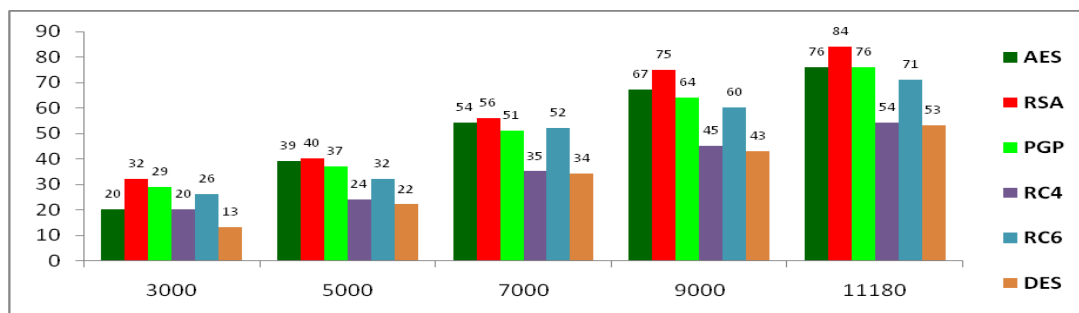


Figure 1: Comparison graph for encryption time taken by different algorithms

.From the figure 1 it is clear that the DES takes less encryption time compare to other algorithms in three layer architecture.

Table3 shows the CPU Utilization Ratio of different algorithms.

Table 3: CPU Utilization by different algorithms

File Size In kb	CPU Utilization Ratio					
	AES	RSA	PGP	RC4	RC6	DES
3000	60	62	56	44	55	41
5000	64	66	60	46	60	45
7000	69	71	64	47	67	46
9000	78	81	73	58	74	56
11180	90	92	81	66	78	61

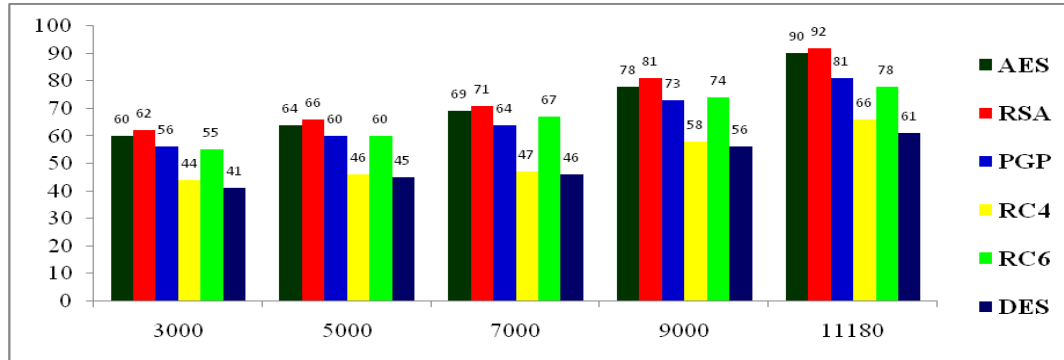


Figure 2: CPU Utilization Ratio of different algorithms

From Figure 2, it is clear that the CPU Utilization of DES algorithm. In three layer distributed architecture is better than other algorithms

Table 4: Memory Utilization by different algorithms

File Size In kb	Memory utilization in kb					
	AES	RSA	PGP	RC4	RC6	DES
3000	1102	995	1005	1061	1010	980
5000	1119	1004	1054	1090	1054	1042
7000	1133	1180	1105	1110	1083	1061
9000	1250	1303	1121	1141	1105	1090
11180	1272	1320	1135	1161	1126	1125

From figure 3, it is clear that the Memory Utilization of DES algorithm is better than other algorithms.

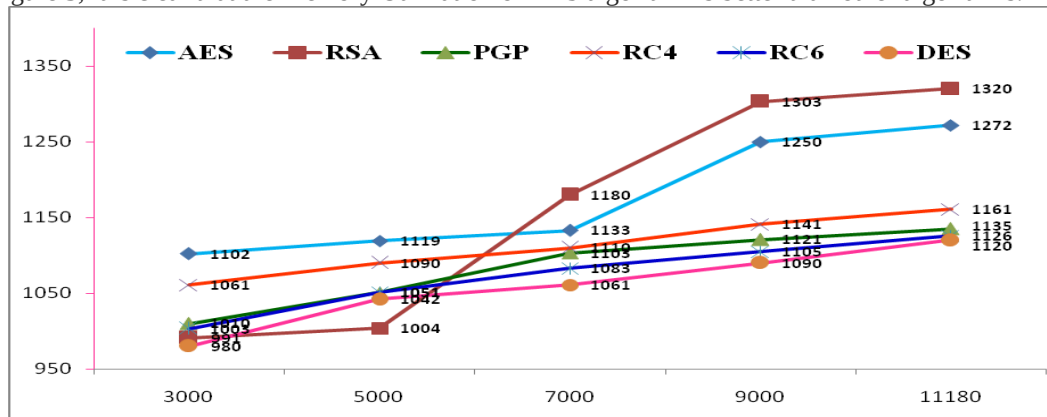


Figure 3: Memory Utilization ratio of different algorithms.

V. Conclusion

There are six popular algorithms are taken in this study and from experimental results it is found that DES provides better result compared to another algorithms in respect to CPU Utilization, Memory Utilization and Encryption time. Although DES is a Slow encryption scheme but in three layer architecture it gives better results compared to another encryption scheme.

References

1. P.Princy(2015), "A comparison of Symmetric Key Algorithm DES, AES, BLOWFISH, RC4, RC6: A Survey", International Journal, 6(5), pp.328-331.
2. S C Rachana, Dr. H S Guruprasad, (2014), "Emerging Security Issues and Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology, 3(2).
3. Vineet Kumar Singh, Maitreyee Dutta (2014), "Analyzing Cryptographic Algorithm For Secure Cloud Network", International Journal of advanced studies in Computer Science and Engineering, 3(6).
4. Priyanka Arora, Arun Singh, Himanshu Tyagi (2012), "Evaluation and Comparison of Security Issues on Cloud Computing Environment", in World of Computer Science and Information Technology Journal, 2(5), pp.179-183.

5. Perna Mahajan & Abhishek Sachdeva(2013), "A Study of Encryption Algorithms AES, DES and RSA for Security ", Global Journal of Computer Science and Technology Network Web & Security,13 (15).
6. Yogesh Kumar, Rajiv Munjal and Harsh Sharma(2011),"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", International Journal of Computer Science and Management Studies,11(3).
7. Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz(2016),"Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering,6(3),pp.659-665.