Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java

Shraddha Dadhich
Department of Computer Science & Engineering
Poornima Institute of Engineering and Technology, Jaipur, India

Abstract- *In the era of science, security is one of the most important part of communication. As in "Smart City" data transmission takes place, so to make that data secure, Cryptography is used. Firstly data which is transmitted by sender is encrypted by encryption techniques. Secondly, receiver can get the original data by using decryption techniques. In Cryptography encryption and decryption of data is done by using secret key which provides data confidentiality, data integrity and data authentication to user. This paper provides the comparative study and performance analysis of AES and DES cryptographic algorithms on two different operating systems using JAVA.*

Keywords: *Cryptography, AES, DES, Smart City.*

I. INTRODUCTION

In recent years, several applications, based on internet, used for communication purpose, needs end to end secure connection. Many companies are collaborating with government to make everything digital so that people can do their work from home also but all these facilities provided by the government and private companies need to be secure from attackers or professional hackers. So we can say that today's era is fully automatic in terms of doing work with the help of internet, after some years there won't be any need to do any communication or any manual work. Everything would be digitized in cities. As these cities can be named as "Smart Cities".

"Smart City", as the name suggests, a city equipped with smart devices. In Smart City, communication is one of the important part. Data transmission takes place when communication is done between two or more people or in financial and commercial sector also. When two or more people will communicate through the internet then the data will transmit over the transmission channel. On that transmitted data or on the computer systems which are used for information sending or receiving, any attack by hackers or attackers, is possible. The attacker or hacker use a variety of techniques and tools to get the original information from that transmitted data. It may leads to many catastrophic result also. So we can say "Data security has become a critical facet of smart city". To make prone transmitted data secured from attackers, we need to enhance the security of data that will provide data confidentiality as well as data authentication to user. Security of information will increase with the help of cryptographic mechanism.

Cryptography, a word from Greek origin, means "Secret Writing". Cryptography allows information to be sent in a secure form in such a way that only authentic person will able to retrieve the information. If any attacker attacked on transmitted data and gets the information then he would not be able to get the original information because that data would be in encrypted form and that can decrypted by the authenticated user only. In cryptography, security is provided to both, the sender's and the receiver's end.

In cryptography, at sender's end, when user wants to send a message to receiver, then that original message is known as plain text, which is encrypted before sending over the transmission channel. The message after encryption is known as cipher text or encrypted text which transmits over the transmission channel. At receiver's end, when cipher text is received then it is decrypted into original plain text.

For encryption and decryption of messages different-different algorithms are used which are categorized on the bases of key used for encryption and decryption purpose. Cryptography is categorized into two types that are symmetric key cryptography and asymmetric key cryptography.

This paper provides details of the performance analysis of symmetric key algorithms which includes AES and DES on two different platforms that are WINDOWS and UBUNTU, using JAVA.

A. AES Algorithm

National Institute of Standards and Technology recommended Advanced Encryption Standard (AES) as the new encryption standard to replace Data Encryption Standard (DES) in year 2001

[1]. In AES algorithm, input is of 128 bits and key size could be of either 128, 192 or 256 bits. Depending on the key length, this algorithm is referred as AES-128, AES-192 or AES-256 [1].

In AES algorithm, we decide the rounds on the basis of key length, such if the number of rounds is 10 a 128 bit key size will be used, if the number of rounds is 12 rounds a 192 bit key size and for 14 rounds a 256 bit key size is used in order to deliver the cipher text or retrieve the plain text. In AES, 128 bit data, divided into four operational blocks, are treated as array of bytes. These all organized as a matrix of the order of 4x4 that is known as “State”.

Initially plain text goes into the first stage that is Add Round Key (figure-1) stage. After that the output of first stage goes through nine main rounds, before reaching the final round. In each round there is four transformations which are performed are as following as:-

1. Sub-bytes
2. Shift-Rows
3. Mix-columns
4. Add round key

In the last round there is no Mix-Column transformation. The output of last round is the cipher text.

In order to get the plain text from the cipher text, inverse functions is used that are Inverse Sub-Byte, Inverse Shift Rows and Inverse Mix Columns.

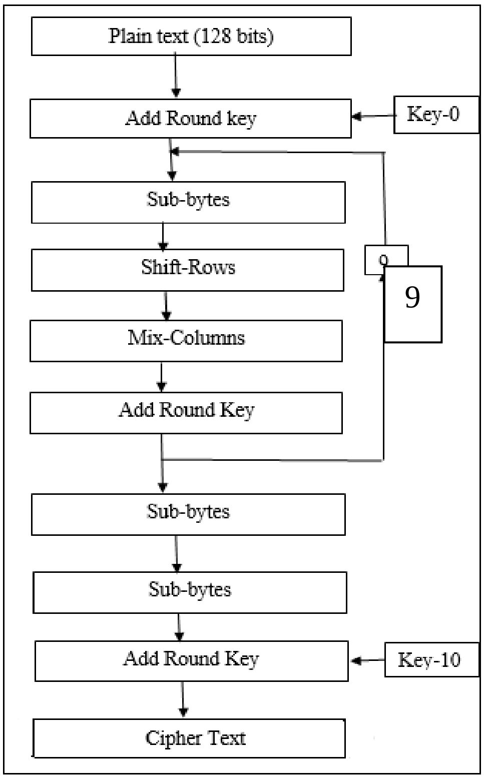

Figure 1. General Depiction of AES

Transformations which are used in each round:-

1. Substitute Byte Transformation: - AES contains 128 bit input data block. In this, the size of each block is 16 bytes. In sub-byte transformation, each byte that is 8-bit of a data block is transformed into another block with the help of 8-bit substitution box which is known as Rijndael Sbox [1].
2. Shift Rows Transformation: - It is a simple byte transformation. Bytes in the last three rows are dependent upon the row location and are cyclically shifted left in this transformation. 1 byte circular left shift is performed for 2nd row. For 3rd and 4th row 2-byte and 3-byte circular left shifts are performed respectively.
3. Mix Columns Transformation: - This round is equivalent to a matrix multiplication of each column of the states. Each column vector is multiplied by a fixed matrix. In this operation the bytes are taken in polynomial form rather than numbers.
4. Add Round Key Transformation: - It is a bitwise XOR between the present state and the round key of 128 bits. This transformation is its own inverse.

B. DES Algorithm

DES refers to Data Encryption Standard which is a United States government standard encryption algorithm for encrypting and decrypting unclassified data [2]. DES is developed by IBM in 1970s.

It is later adopted by National Institute of Standards and Technology (NIST) as Federal Information Processing Standards (FIPS 46) [1]. The most recent revision is “FIPS 46-3.1” [1]. DES is based on IBM’s Lucifer cipher [1].

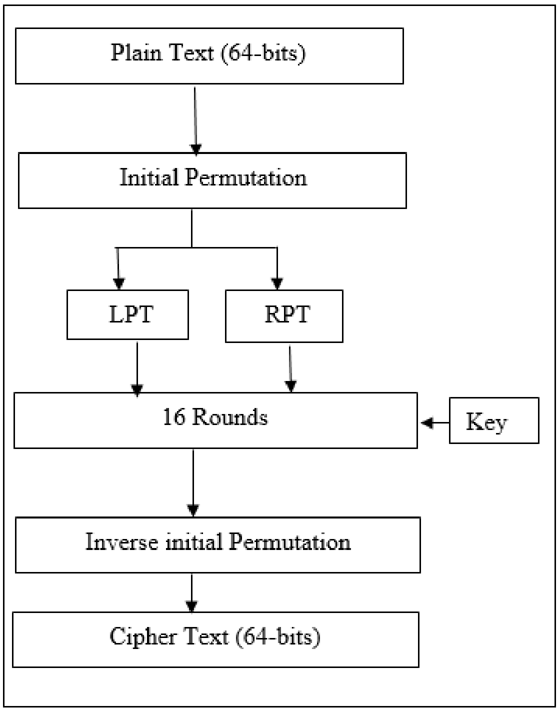

Figure 2. General Depiction of DES

DES is a block cipher. It takes input in the form of plain text and creates a cipher text string of the same length. It uses same key for encryption and decryption that is why key is known as symmetric key. It is a symmetric block cipher which takes 64-bits long input but only 56-bits key with 8-bits of parity for error detection in encryption and decryption. The algorithm is open but the key is not released that's why the information security is fully dependent on secrecy of the key. Data Encryption Standard algorithm synthetically makes use of many cryptography technologies which include replacement, alternation and data input [1]. It is a product cryptogram.

In this algorithm, plaintext is divided into many blocks when encryption begins. Each block is of 64 bits and the length of key is also 64 bits. The valid length of key is 56 bits and the rest 8 bits are used as parity bits for error checking. Firstly, 64 bits data is divided into two parts after initial permutation that are LPT and RPT. Each part includes 32 bits. Then iterative process began, firstly, RPT which is of 32 bits is extended to 48 bits and after that exclusive-or operation is performed with 48 bit key which is got from 56 bit key. After that result is compressed as 32 bits through s-box. After replacement, the 32 bit data exclusive-or with LPT which is of 32 bits taken from the beginning of replacement with RPT. RPT of the new round is determined. After 16 round replacements, a new 64 bit data is generated. There is one step we need to pay attention that is "The two results of last round do not exchange". At last, the 64 bit result needs an inverse initial permutation, resulting to the 64 bits cipher text.

In order to get plain text from cipher text, cipher text will be now passed as an input. After that same process will happen but key will be used in the reverse order, that is, key-16 will be used in first round, key-15 will be used in second round and so on until the last round.

II. RELATED WORK

Previously, many researches have been done under the topic cryptography in security. They have introduced algorithms for security purpose as well as they have analysed the performance of those algorithms with respect to encryption and decryption time.

As we know, security is prime point of concern in today's era, so in this regard, this section will give you brief about the previous researches on security in Smart City.

In 2013, Dr. Prerna Mahajan *et al.* [2] presented an analysis on performance of AES, DES and RSA on the basis of stimulated time for encryption and decryption [2].

In 2015, Nivedita Bisht *et al.* [3] presented a comparative study of some symmetric and asymmetric key cryptographic algorithms.

In 2012, Mandal *et al.* [6] presented a paper. This paper discusses the comparison between two symmetric encryption technique which are used widely i.e. data encryption standard (DES) and advanced encryption standard (AES) on the basis of avalanche effect due to one bit variation in plaintext keeping the key constant, memory required for implementation and simulation time required for encryption.

A significant change in the key as well as plain text should produce a small significant change in the cipher text, this is known as Avalanche effect [6].

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in ciphered text}}{\text{Number of bits in ciphered text}}$$

Avalanche effect is very high for AES as compared to DES whereas memory requirement and simulation time for DES is greater than that of AES, which shows AES is better than DES.

For encryption of messages between objects sent over chat-channels, AES is ideal and is useful for objects that involve monetary transactions [6].

In 2013, Sumitra [4] has done the performance analysis of AES and DES on different-different machines and gave conclusion that is different machines take different times for same algorithm over same data packet [4].

In 2013, Gurpreet Singh and Supriya has presented a survey of various encryption techniques and concluded the result that is AES algorithm is most competent in terms of speed, time, through-put and avalanche effect [5].

III. COMPARATIVE STUDY OF AES & DES

In table-1, comparative study of AES & DES has been shown on the basis of different factors like key size, block size, encryption, decryption, speed, security and etc.

Table 1: Theoretical analysis of AES and DES

Input String	**Operating System**	**Total time taken in AES (In nano sec.)**	**Total time taken in DES (In nano sec.)**
hello	Windows	14926660	16815574
	Ubuntu	11338436	14389933
GOOD	Windows	12082968	17928377
	Ubuntu	11023252	13505159
Good	Windows	13462579	18227735
	Ubuntu	12158347	14643395
12345	Windows	13277602	18626904
	Ubuntu	11391367	13123996
@#$	Windows	13245428	18102303
	Ubuntu	10014221	14210172
A123	Windows	12587960	17351110
	Ubuntu	12126571	13334279

IV. EXPERIMENTAL RESULT & ANALYSIS

As security is one of the major issue in today's era so to enhance security we have cryptographic algorithms. In this paper, implementation of AES and DES cryptographic algorithms on two different platforms like WINDOWS and UBUNTU using JAVA has taken into consideration. By this implementation, performance analysis of these two algorithms has completed. Performance of these two algorithms depends upon various factors like no. of rounds, key size and etc., but in this experimental analysis performance is evaluated considering two parameters:-

1. Encryption Time
2. Decryption Time

As we know, Encryption time is the time taken by the algorithm to produce the cipher text and Decryption time is the time taken by algorithm to produce plain text from cipher text.

Experimental results for cryptographic algorithms AES and DES are shown in table-2, which shows the comparison of speed of these two algorithms i.e. AES and DES, using same input string.

By analysing table-2, time taken by DES algorithm for encryption and decryption is more than AES algorithm for the same input. So we can say that AES algorithm is fast with comparison to DES algorithm.

On the basis of these results we can analyse the performance of AES and DES on various operating systems also, for example when comparing WINDOWS and UBUNTU both the algorithms execute much faster in Ubuntu than Windows.

Table 2: Comparative study of AES and DES total stimulated time

Factors	**AES**	**DES**
Developed By	Vincent Rijmen, Joan Daemen	IBM
Developed in year	2001	1970's
Key Size	128,192,256 bits	56 bits
Block Size	128 bits	64 bits
Encryption	Faster	Comparatively Slower
Decryption	Faster	Comparatively Slower
Speed	Fast	Slow
Security	More Secured	Not Secure Enough
Rounds Used	10/12/14 rounds	16 rounds
Key used	Same key used for encrypt and decrypt	Same key used for encrypt and decrypt
Algorithm	Symmetric Algorithm	Asymmetric Algorithm

V. FUTURE WORK

In future, we can take the remaining parameters like no. of rounds, key size, etc. for performance analysis of algorithms.

Our future work will explore this implementation with different-different languages like VHDL, C etc. and implementation will be done on different-different operating systems. After analysing the performance of algorithms, a combination of algorithms can be applied in parallel manner or sequential manner to make a set-up which will provide more security to data storage and retrieval.

VI. REFRENCES

[1] Atul kahate, Cryptography and network security (New Delhi, Tata McGraw hill publication, 2010)

[2] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", IITM India in Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013.

[3] Nivedita Bisht & Sapna Singh, "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms, Assistant Professor, Department of Electronics and communication Engineering, SIT Pithoragarh, India in International Journal of Innovative Research in Science, Engineering and Technology, (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2015.

[4] Sumitra, "Comparative Analysis of AES and DES security Algorithms ",Lecturer (Computer science) Advanced Institute of Technology & Management, Palwal in International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013.

[5] Gurpreet Singh & Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", M.Tech Research Scholar, Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India in International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013 Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013.

[6] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.