**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 9, September 2014, pg.582 – 585***

**RESEARCH ARTICLE**

# Performance Evaluation of Cryptographic Algorithms: AES and DES

**Divya Sukhija**

Student at JCD College of Engineering, India

divya.sukhija@gmail.com

***Abstract— Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Cryptography is the process where an individual or message sending by party to other individual such that only the authorize party will get the scrambled message, which will be unscrambled to get the original message. The purpose of cryptography is to secure the data so that it cannot be accessed by any unauthorized party. The plain text is converted into an unreadable form known as cipher text. This process is known as Encryption. The encrypted text is converted back into original text and this process is known as Decryption***

***Keywords— Cryptography, Encryption, Decryption, AES, DES***

## I. INTRODUCTION

CRYPTOGRAPHY

Cryptography is basically the process of hiding information. Our ATM cards, Computer passwords and transferring data from one place to another are done with cryptography. Cryptography is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Data cryptography mainly is the scrambling of the content of data, such as text, image audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data Decryption.

Original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer. Whereas the data, which is unreadable, neither human nor machine is called cipher text. A system or product that provides encryption and decryption is called cryptosystem.


**Cryptography Goals:**

There are five main goals of cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system.

 

These goals can be listed under the following five main categories:

- **Authentication:** The process of proving one's identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
- **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.
- **Non-repudiation:** A mechanism to prove that the sender really sent this message. Means that neither the sender nor the receiver can falsely deny that they have sent a certain message.
- **Service Reliability and Availability:** Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

## II. DATA ENCRYPTION STANDARD (DES)

**Brief History of DES:**
DES (and most of the other major symmetric ciphers) 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. Most symmetric encryption schemes today are based on this structure (known as a **feistel network**).As with most encryption schemes; DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of cipher it is. DES is therefore a symmetric, 64 bit **block cipher** as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time5 (be they plain text or cipher text). The key size used is 56 bits, however a 64 bit (or eight-byte) key is actually input. The least significant bit of each byte is either used for parity (odd for DES) or set arbitrarily and does not increase the security in any way. All blocks are numbered from left to right which makes the eight bit of each byte the parity bit. Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. Multiple permutations and substitutions are incorporated throughout in order to increase the difficulty of performing a cryptanalysis on the cipher.

## III.ADVANCED ENCRYPTION STANDARD (AES)

It is a symmetric key encryption standard adopted by the in US government in 2001. It was designed by Vincent Rijmen and Joan Daemena in 1998 later inspected by National Institute of Standards and Technology (NIST) as U.S. FIPS in November, 2001. Various security checks had been performed in the procedure and AES was declared the best encryption standard out of 12 participated standards and the use of AES becomes effective in May, 2002. It has 3 different key sizes: 128, 192 and 256 bits used for the encryption of the 128 bit block size data. It includes three different default rounds depending upon the key length i.e. 10 for a 128 bit key size, 12 for a 192 bit key size and 14 for a 256 bit key size.
The algorithm is designed to use keys of length 128, 192 or 256. It works on one block of 128 bits at a time, producing 128 bits of cipher text. There are 10 rounds, after an initial XOR'ing (bitwise addition mod 2) with the original key (assuming a key length of 128). These rounds, except for the last, consist of 4 steps (layers), called Byte Sub, Shift Row, Mix Column and Add Round Key. In the 10th round the Mix Column step is omitted. The 128 bit input is divided into 16 bytes of 8 bits apiece. These are arranged in a 4 × 4 matrix. The Shift Row and Mix Column steps operate on this matrix while the Byte Sub and Add Round Key steps just operate on the bytes.

The steps followed in AES are:
• **Sub Bytes()**
• **Shift Rows()**
• **Mix Columns()**
• **AddRoundKey()**

 

**STRENGTH AND WEAKNESS:**

**Advanced Encryption Standard (AES):**

- AES is highly efficient, secure and it is not complex.
- It needs more processing.
- It requires more rounds of communication as compared to DES.

**Data Encryption Standard (DES):**

- DES has been around a long time since1978. and has been studied to death.even now no real weakness have been found.
- The most efficient attack is still brute force.The 56 bit key size is the biggest defect.
- Hardware implementations of DES are very fast; DES was not designed for software and hence runs relatively slowly.

## IV. TOOLS USED

**CRYPTOOL 1.4.31 :**

- Freeware program with graphical user interface.
- Cryptographic methods can be applied and analyzed.
- Comprehensive online help (understandable without deeper cryptography knowledge).
- Contains nearly all state-of-the-art cryptography functions.
- Easy entry into modern and classical cryptography.
- Not a *"*hacker tool*"*.

**Why CrypTool?**

- Origin in awareness initiative of a financial institute.
- Developed in close cooperation with universities.
- Improvement of university education and in-firm training.

**Target group**

- Core group: Students of computer science, business computing and mathematics.
- But also for: computer users, application developers, employees.
- Prerequisite: PC knowledge.
- Preferable: Interest in mathematics and/or programming.

**Description:**

Modern communication requires secure encryption methods. Today, an exorbitant amount of information is transmitted via the internet. Millions of people use websites for their banking activities causing the transmission of sensible data via networks where the precise routing of data is not always known and data may be manipulated or stolen. Further examples of daily usage of data encryption are mobile phones and wireless networks. In the past, somebody who wanted to encrypt data had to deal directly with the process and was therefore aware of the process. Today, however, this process runs usually fully automated in the background, so that the user does not perceive it. Nevertheless uneducated users may easily fail to use these mechanisms in a secure manner.

## V. CONCLUSION

In this paper we have compared cryptographic algorithms AES and DES by using the tool **CRYPTOOL 1.4.31 .**The comparison is done by using the parameters Binary Histogram, Autocorrelation and Floating Frequency. Based upon these parameters it is concluded that AES is better than DES.

 

**REFERENCES**

[1] N.Penchalaiah (2010)**"**Effective Comparison and evaluation of DES and AES.**"(**International Journal of Computer Science and Engineering)volume 2.

[2] Majithia Sachin (2010) **"**Implementation and Analysis of AES, DES and Triple DES on GSM Network.**"(** International Journal of Computer Science and Network Security), VOL.10.

[3] Ayushi(2010) **"**A Symmetric Key Cryptographic Algorithm**" (**International Journal of Computer Science Applications)Volume1.

[4] Sandipan Basu(2011) **"**International Data Encryption Algorithm(IDEA)**" (**Journal of Global Research in Computer Science)Volume2.

[5] D.kumar,V.Chahar(2011)**"**Performance Evaluation of DWT based Image Technography.**"** (IEEE Second International Conference on Advanced Computing).

[6] S.Pavithra (2012) **"** Study and performance analysis of cryptographic algorithms**."**( ISSN*:* 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology)Volume 1, Issue 5, July 2012**.**

[7] Ajay kakkar(2012)**"**Comparison of Various Encryption Algorithms and Techniques for secured Data Communication in Multinode Network**"** (International Journal of Engeneering and Technology) Volume 2 No. ISSN: 2049-3444 © 2011 – IJET.

[8] Andrew(2012) Cryptography: **"**A Comparison of Public Key System.**"**

[9] Shraddha Soni (2012)**"**Analysis and Comparison between AES and DES Cryptographic Algorithm**"(**International Journal of Engineering and Innovative Technology).

[10] Nagesh kumar (2012) **"**Performance analysis of symmetric key cryptography. Algorithms: DES, AES and BLOWFISH**"** (International Journal of Engineering and Innovative Technology) (IJEIT) Volume 2, Issue 6, December 2012 362.

[11] Mohit Marwaha (2013) **"**Comparative analysis of cryptographic algorithms.**"**(International Journal of Advanced Engineering Technology) E-ISSN 0976-3945.

[12] Ali Makhmali(2013)**"**Comparative Study of Cryptographic Algorithm and Proposing a Data Management Structure**"(**International Journal of Scientific & Technology)ISSN 2277-8616 Volume 2.

 