"COMPARATIVE STUDY OF AES AND DES ALGORITHM IN NETWORK PACKET SWITCHING"

[1]SWATI D. KADU
PG Department of Computer Science & Technology HVPM, Amravati, India
Swatikadu17@gmail.com

[2]DHANASHRI A. PATHAK
PG Department of Computer Science & Technology HVPM, Amravati, India
dnpathak24@gmail.com

[3]DR. S. P. DESHPANDE
PG Department of Computer Science & Technology HVPM, Amravati, India
shrinivasdeshpande68@gmail.com

1. INTRODUCTION

A network is simply a group of two or more Personal Computers linked together. Many types of networks exist, but the most common types of networks are Local-Area Networks (LANs), and Wide-Area Networks (WANs). Networks are usually classified using three properties: Topology, Protocol and Architecture. [1] Topology specifies the geometric arrangement of the network. Protocol specifies a common set of rules and signals the computers on the network use to communicate. .

2. THE TCP/IP MODEL

TCP/IP defines a set of rules to enable computers to communicate over a network TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet.

The TCP/IP Model is a specification for computer network protocols. TCP/IP defines a set of rules to enable computers to communicate over a network. It specifies how data should be formatted, addressed, shipped, routed and delivered to the right destination.

2.1 TCP/IP describes the top 4 layers

The first layer is called the Physical layer. This layer is responsible for encoding and transmitting data over network communications media. It operates with data in the form of bits which are sent from the Physical layer of the sending source and received at the Physical layer of a destination source. When you hook up a computer using an Ethernet cable you are connecting that computer on the Physical layer. This Physical layer is the lowest level of the TCP/IP Model.

The next layer is the Data link layer. This layer is used to move packets from the network layer on two different hosts. The process of transmitting packets on a link layer can be controlled in the software device driver for the network card and on firmware. The next layer is the Network or Internet layer. This layers gets data from a source network to the destination network. This generally involves routing the packets across a network . In this IP performs the basic task of getting packets of data from source to destination.

The next layer is the Transport layer. The transport layer's responsibility is end-to-end message transfer. There are 2 categories of end-to-end message transmission: connection-oriented (TCP) or connectionless (UDP). The transport layer provides this service of connecting applications together through the use of ports. This layer offers reliability and error control.

The fifth and final layer is the Application layer. This layer refers to higher-level protocols used by most applications for network communication. An example of application layer protocol is FTP (File Transfer Protocol). [1]

3. IP PROTOCOL

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for:

- **IP addressing** - The IP addressing conventions are part of the IP protocol.
- **Host-to-host communications** - IP determines the path a packet must take, based on the receiving host's IP address.
- **Packet formatting** - IP assembles packets into units known as **IP datagrams**. Datagram's are fully described in "Internet Layer".
- **Fragmentation** - If a packet is too large for transmission over the network media, IP on the sending host breaks the packet into smaller

fragments. IP on the receiving host then reconstructs the fragments into the original packet.

3.1 ICMP Protocol

Internet Control Message Protocol (ICMP) is the protocol responsible for detecting network error conditions and reporting on them. ICMP reports on:

- Dropped packets (when packets are arriving too fast to be processed)
- Connectivity failure (when a destination host can't be reached)
- Redirection (which tells a sending host to use another router) .[1]

Encryption:

Encryption is method of storing and transmitting data in form that only those it is intended or can read and process. Encryption is an effective wave of protecting sensitive information as it is stored on media or a transmitted through network communication path.

There are two types of Encryption

1. Symmetric Key
2. Asymmetric Key

Symmetric Key: Symmetric key also called as private key or secret key. Encryption uses same key to encrypt and decrypt. The name "Private key" derives from the need to keep key private. Common symmetric key encryption algorithm includes DES (Data Encryption Standard) and AES (Advanced Encryption Standard)algorithm.

Asymmetric key: Asymmetric key also called public key encryption. Uses two key public key and private key. Data encryption with one key can be decrypted only with other key.[2]

4. PACKET TRACER

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. Packet Tracer can be run on IOS, Linux and Microsoft Windows. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a "cable" item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Cisco Systems claims that Packet Tracer is useful for network experimentation. Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. Packet Tracer can be run on IOS, Linux and Microsoft Windows. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a "cable" item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. . Cisco Systems claims that Packet Tracer is useful for network experimentation. [3]

5. LITERATURE REVIEW

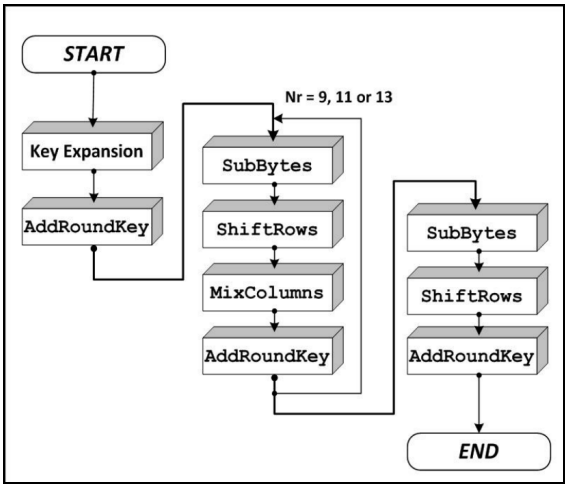
AES and DES both Algorithms consume different time at different machine. Different machine take different time for same algorithm over same data packet. Algorithms show different speed in packet transfer. AES is more secure as compare to DES. In this paper AES algorithm take minimum time to send packet as compare to DES algorithm. [5]

Longer key length and a data length consume more power and it result in more heat dissipation so it is not advisable to use short data sequence and key length because by using power full software one can hack short keys very easily an able to break the system.[6]

By comparing the various factors of the AES and DES algorithm that are (key length, cipher type, block size, developed, cryptanalysis resistance, security, possible keys, possible ASCII printable character keys, time required to check all possible keys) the AES is better than DES.[7]

5.1 Algorithm Used For Encryption

1. AES Symmetric Encryption



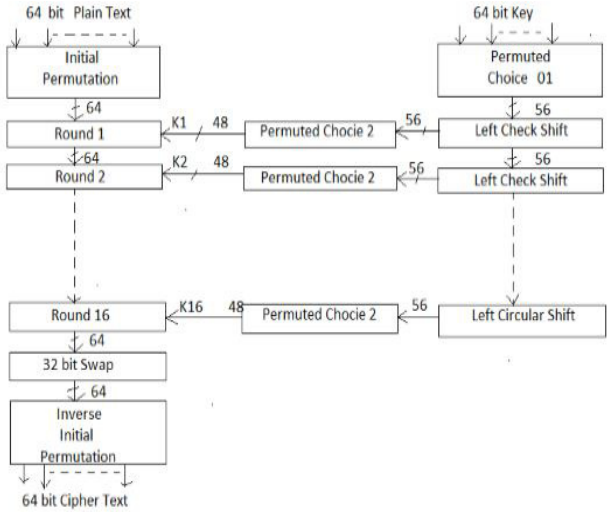
Steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array
4. Perform nine rounds of state manipulation
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

5.2 DES Algorithm

The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. ES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. This is mainly due to the 56-bit key size being too small.

Flowchart for DES:



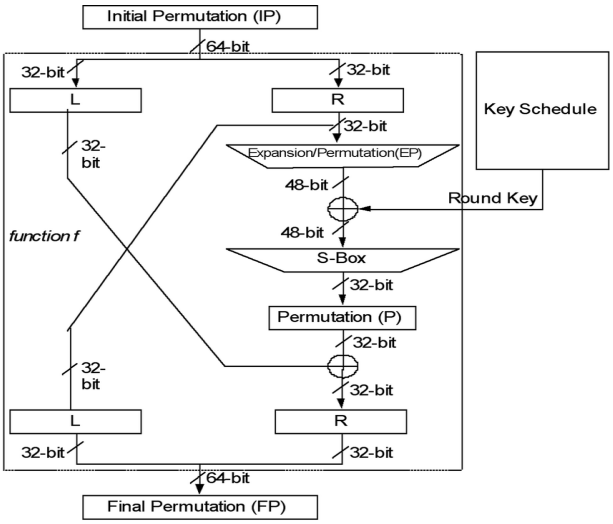
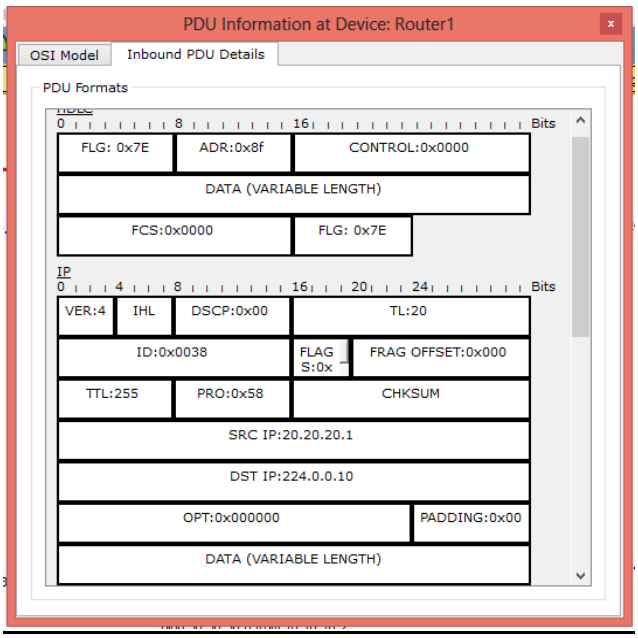


Figure: Round process in DES algorithm

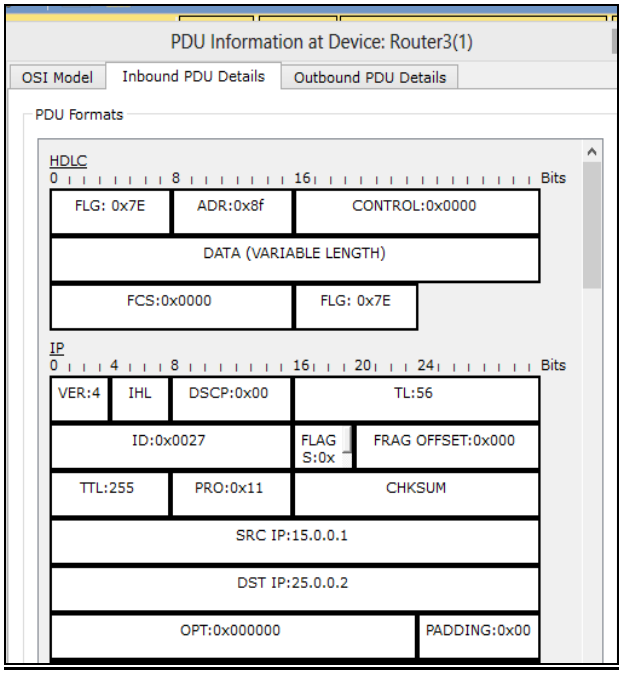
Steps Fractioning of the text into 64 bit blocks.

1. Initial permutation of block.
2. Breakdown of the block into two parts: left and right, named L and R;
3. Permutation and Substitution steps repeated 16 times of DES algorithm:
4. Rejoining of the left and right parts then inverse initial permutation.

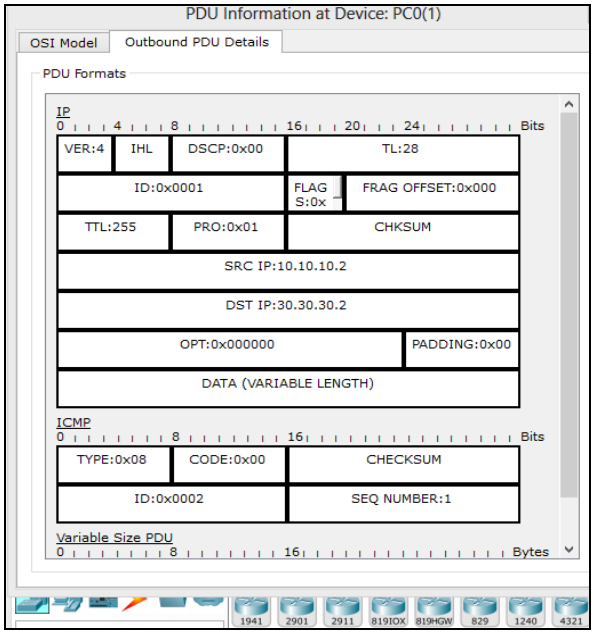
6. RESULT ANALYSIS



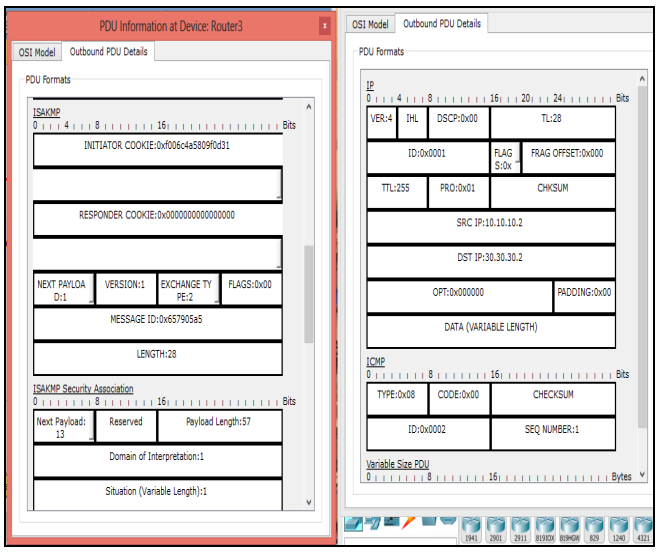
Time to leave simple packet



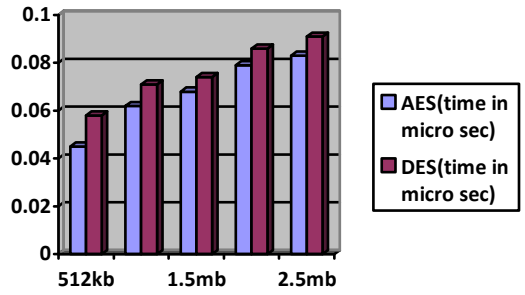
Time to leave encrypted packet



Simple Packet Format



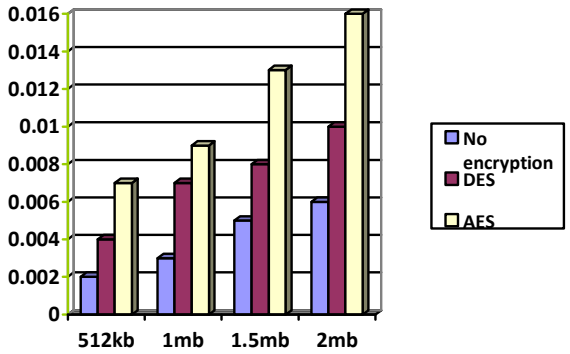
Encrypted Packet Format



Analyzing time based on both algorithm

% Power consumption based on packet size

1W



7. CONCLUSION

From this experiment it is conclude that simple data packet required less time to send data packet as compare to encrypted data packet. It is clear that AES encryption algorithm is more secure than the DES algorithm. Because of the maximum key length it has 256 possible combinations of key.

8. REFERENCE

[1] William Stallings," Cryptography and Network Security" 7th Edition March 5,2016

[2] Behrouz A. Forouzan," Cryptography and Network Security"

[3] WWW.quora.com/What-is-Ciscos-Packet-Tracer

[4] http://en.m.wikipedia.org

[5] Sumitra , "Comparative analysis of AED and DES security algorithm." (International Journal of Scientific & Research Publications, volume 3, Issue 1, Jan 2013, ISSN.2250-3153

[6] Soheila Omer AL Faroog Mohammad Koko, Dr. Amin Babiker A/Nabi Mustafa AL, "Comparison of various Encryption Algorithms and Techniques for improving secured data communication" Neelain university, Faculty of Engineering. Khartoum, Sudan, IOSR Journal of Computer Engineering (IOSR-JCE)

[7] Hamdan.O.Alanazi, B.B.Zaidan, Hamid A. Jalab, M. Shabbir, and Y. AI-Nabhani, "New Comparative Study Between AES,DES and 3DES within nine Factors"(Journal of Computing, Volume2,Issue3,March2010,ISSN:2151-9617