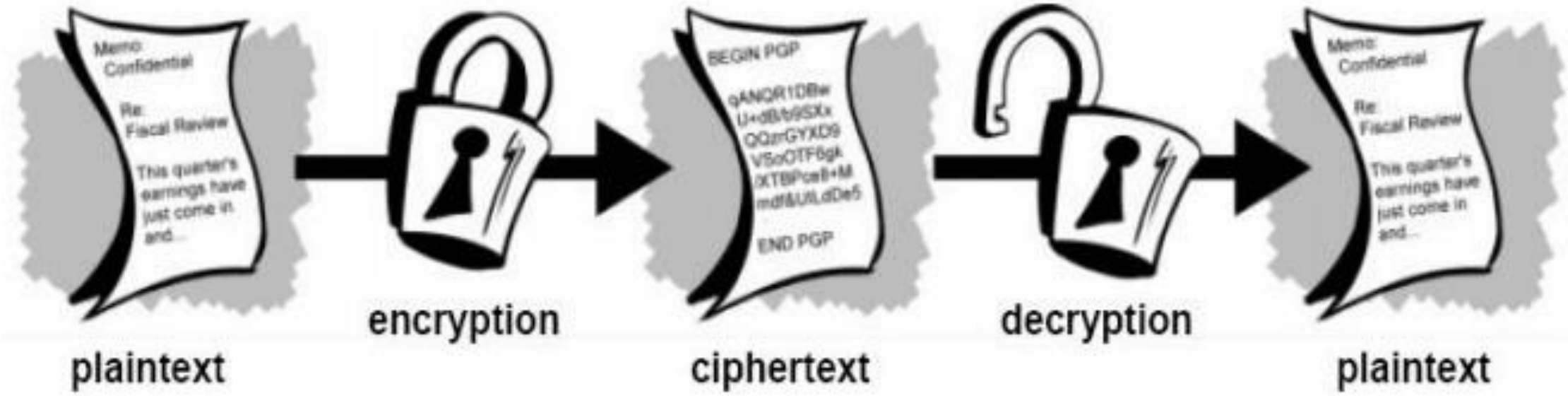
THE DES CRYPTOGRAPHIC ALGORITHM

TEAM MEMBERS	REGISTER NUMBERS
VIGHNESH PRADHAN	RA2011030010180
IMMADISETTY DURGANJANEYULU	RA2011030010176
N.V.PUNEETH SHARAN	RA2011030010184
ARUN YADAV	RA2011030010191

ABSTRACT:

- In this ppt we will discuss the DES technique for secure data transmission while maintaining the authenticity and integrity of the message.
- In this, message is encrypted before the data transmission process starts. The encryption and decryption of data is done by using the data encryption standard algorithm



INTRODUCTION

- Data Security is the main aspect of secure data transmission over unreliable network. The conventional methods of encryption can only maintain the data security.
- DES method is used to store sensitive information or transmit information across insecure networks so that it cannot be read by anyone except the intended recipient.

ALGORITHM:

The algorithm process breaks down into the following steps:

- The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
- The initial permutation (IP) is then performed on the plain text.
- Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
- Each LPT and RPT goes through 16 rounds of the encryption process.
- Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
- The result of this process produces the desired 64-bit ciphertext.

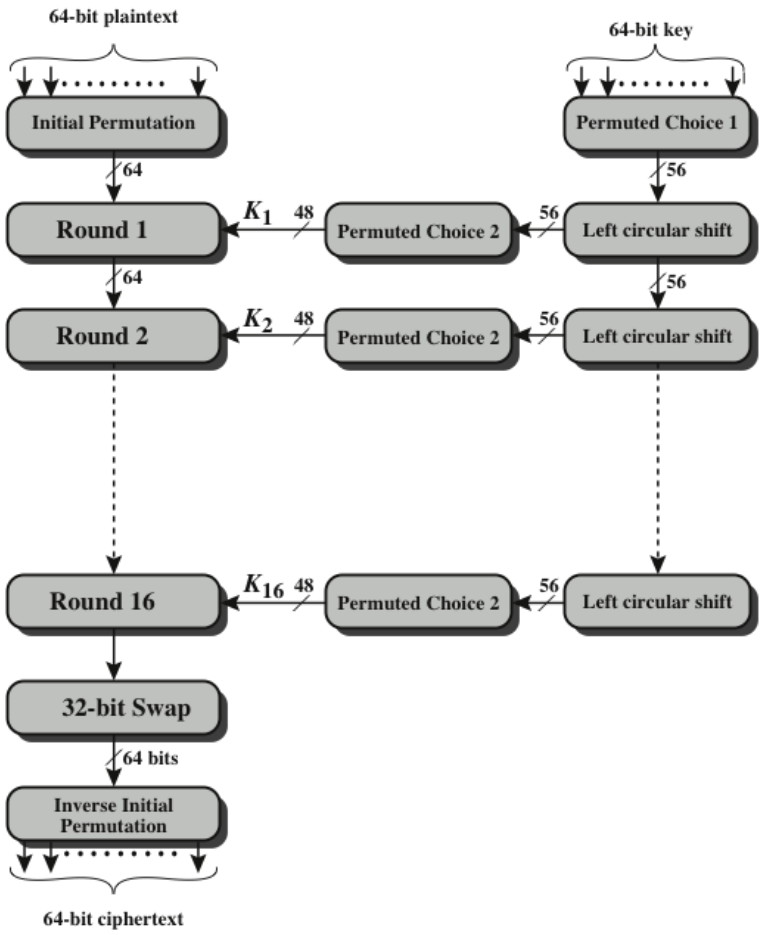


Figure 4.5 General Depiction of DES Encryption Algorithm

Encryption Process:

- The encryption process step (step 4, above) is further broken down into five stages:

Key transformation

Expansion permutation

S-Box permutation

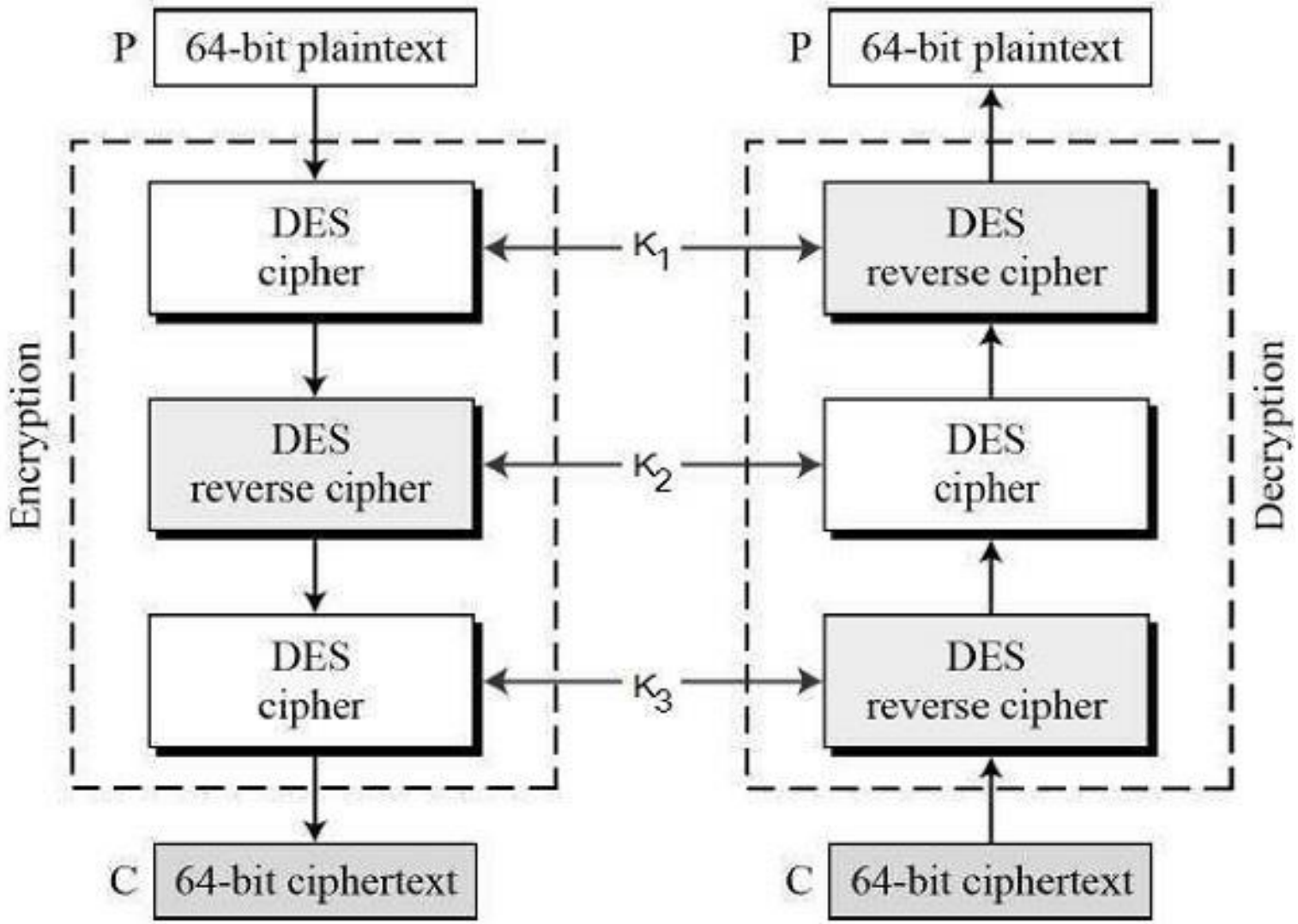
P-Box permutation

XOR and swap

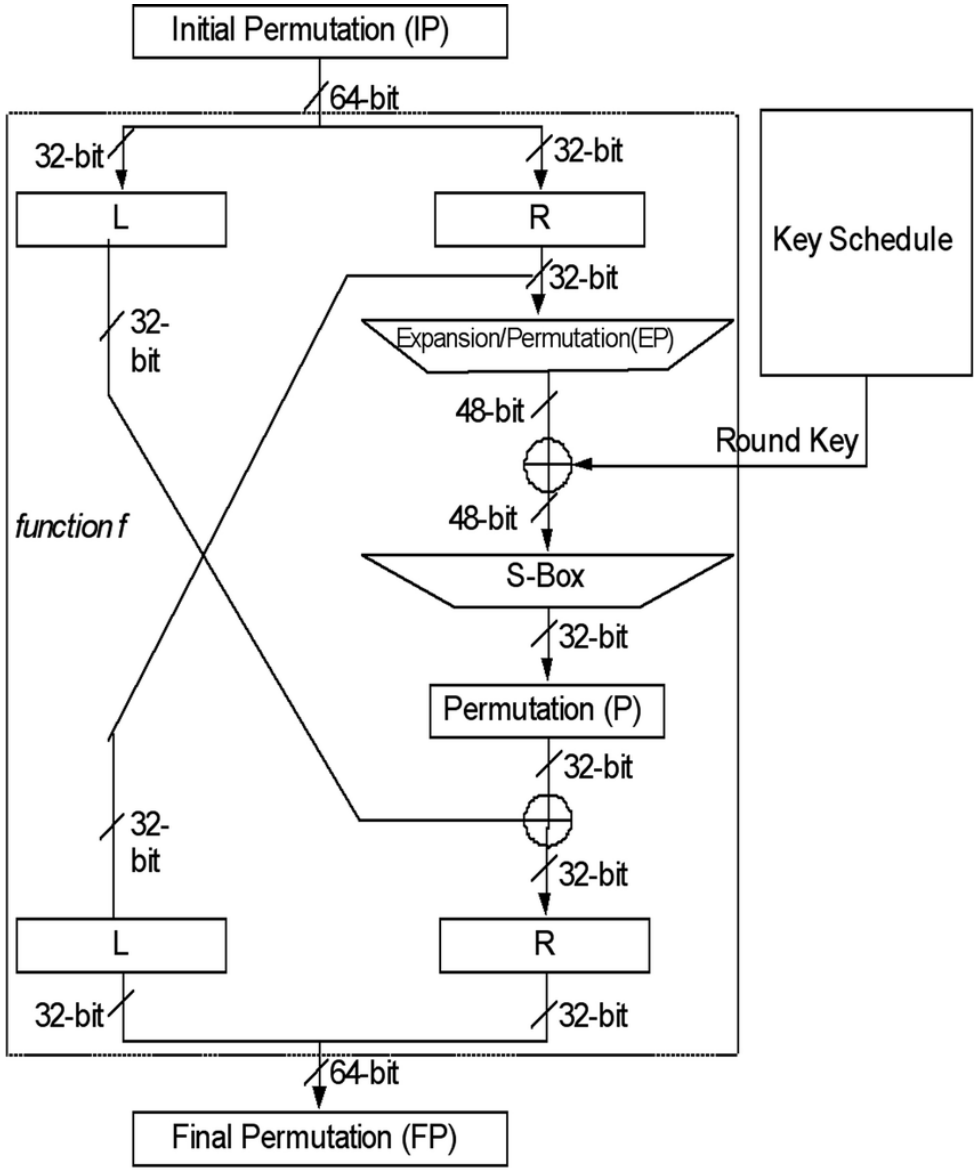
Decryption process:

For decryption, we use the same algorithm, and we reverse the order of the 16 round keys.

Encryption and decryption process steps:



ARCHITECTURE Diagram

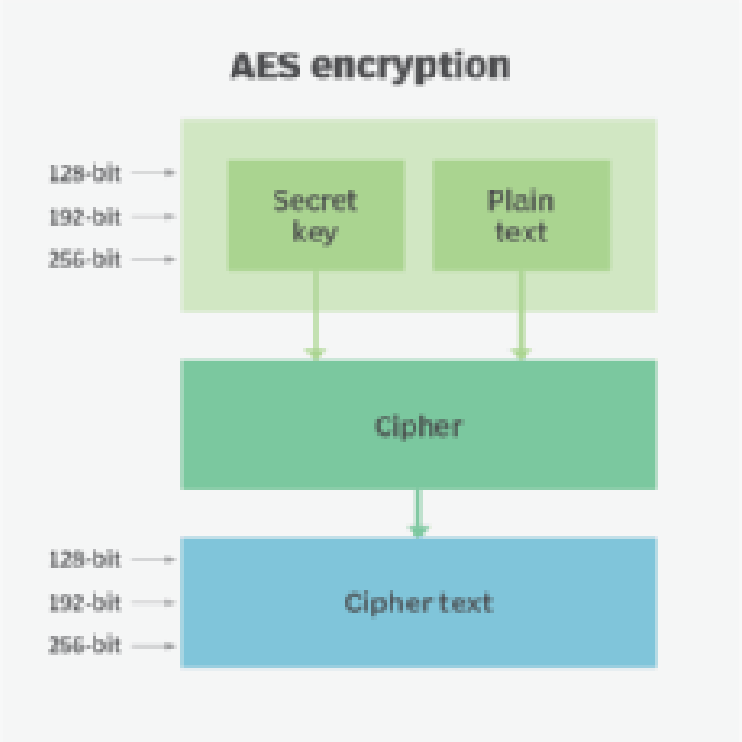


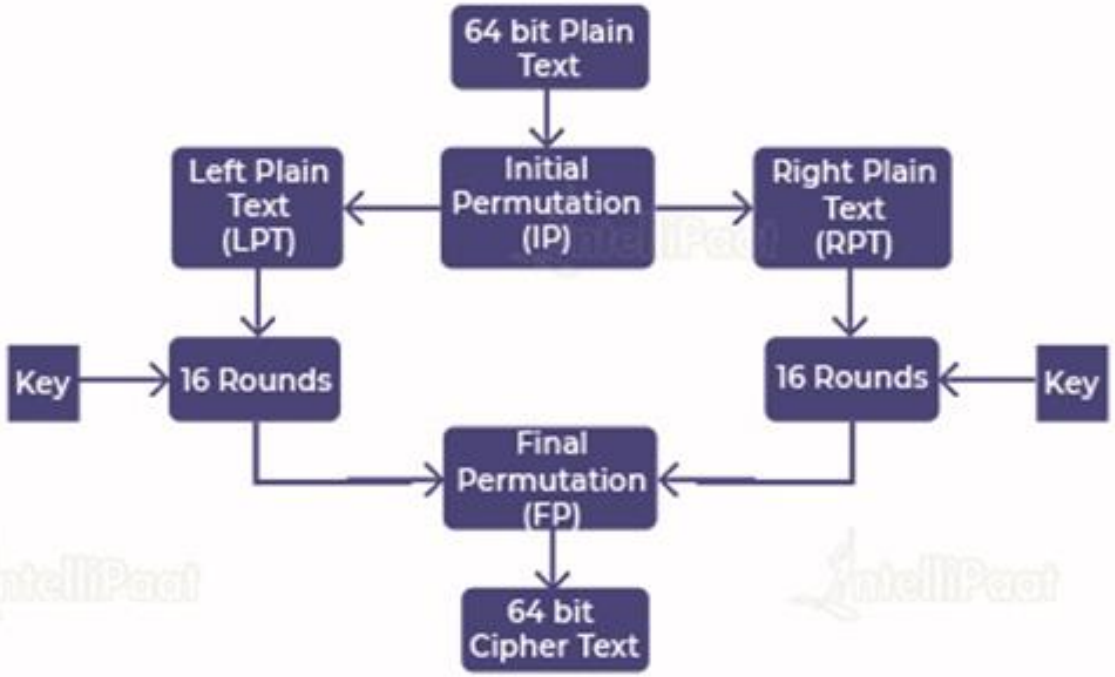
S.N0	TITLE OF THE PAPER	AUTHOR AND JOURNAL NAME	OBJECTIVE OF THE PAPER	METHADOLOGY USED	RESULT OBTAINED	LIMITATION
1.	Data Encryption Standard Algorithm (DES) for Secure Data Transmission	• Nirmaljeet Kaur Research scholar BGIET, Sangrur,India • Sukhman Sodhi Assistant Professor BGIET,Sangrur,India	• DES technique for secure data transmission while maintaining the authenticity and integrity of the message.	• The des algorithm is an block cipher algorithm. This is used to convert the plain text to cipher text	• As we are moving towards the society where automated information resources are very much in use , it is very important to provide a secure mechanism for data transmission.	• The 56 bit key size is the largest defect of DES and the chips to implement one million of DES encrypt or decrypt operations a second are applicable (in 1993). • Hardware implementations of DES are very quick

S.N0	TITLE OF THE PAPER	AUTHOR AND JOURNAL NAME	OBJECTIVE OF THE PAPER	METHADOLOGY USED	RESULT OBTAINED	LIMITATION
2.	DES- Data Encryption Standard	• Indumathi Saikumar Post Graduate Student, Electronic and Communication Engineering, CMR College of Engineering and Technology, Telangana, India	• DES method is used to store sensitive information or transmit information across insecure networks so that it cannot be read by anyone except the intended recipient.	• The des algorithm is an block cipher algorithm. This is used to convert the plain text to cipher text	• Data Encryption Standard has increased the level of security because of the 16 rounds of operation. It is difficult for the unauthorized party to attack and crack	• DES was not designed for application and therefore it runs relatively slowly. • In a new technology, it is improving a several possibility to divide the encrypted code, therefore AES is preferred than DES.

	DES	3DES	Blowfish	AES
Key length	56 bits	112 or 168 bits	448 bits	128, 192, or 256 bits
Block Size	64 bits	64 bits	64 bits	128bits
Developped in	1975	1978	1993	2000
Speed	Slow	Slow	Fast	Fast
Security	Not secure enough	Not secure enough	Secure enough	Excellent security
Structure	Feistel	Feistel	Feistel	Substitution Permutation
Time Required to Check All Possible Keys at 50 billion Keys per second	400 days	800 days	~3200 days	5 x $10^{21} days$

DES encryption vs. AES encryption





Broad Level Steps in DES

DEMO

CONCLUSION

- As we are moving towards the society where automated information resources are very much in use , it is very important to provide a secure mechanism for data transmission. DES is now considered to be an insecure technique of encryption for some applications like banking system. There are some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new level of security to it. In future we can modify this algorithm by modifying the function implementation ,S- box design and replacing the old XOR by new operation .

REFERENCES:

- W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.
- Understanding Cryptography: A Textbook for students and Practitioners by christof Paar, Jan Pelzl , Bart Preneel -2007
- Kumar aman, Jakhar Sudesh & Makkar Sunil, (2012), “Comparative Analysis between DES and RSA Algorithm’s” International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X, vol 2.
- Behrouz A. Forouzan.” Cryptography and Network Security”. Tata McGraw-Hill, 2007.

THANK YOU