**CRYPTOGRAPHY AND NETWORK SECURITY**

**REPORT ON:**

**PARALLEL APPROACH ON DES USING NON LINEAR FEEDBACK SHIFT REGISTER TO AMPLIFY THE SECURITY AND MINIMEZING THE TIME COMPLEXITY**

**SUBMITTED BY:**

ADARSH 4NM17CS0008

ASHWANTH V SHETTY 4NM17CS034

**UNDER THE GUIDANCE OF:**

Mr. Radhakrishna Dodmane

Associate Professor

Dept. Of Computer Science

**NMAM INSTITUTE OF TECHNOLOGY, NITTE**



(ISO 9001:2015 Certified), Accredited with ‘A’ Grade by NAAC

: 08258 - 281039 – 281263, Fax: 08258 – 281265

**Department of Computer Science and Engineering**

B.E. CSE Program Accredited by NBA, New Delhi from 1-7-2018 to 30-6-2021

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

# CERTIFICATE

CRYPTOGRAPHY AND NETWORK SECURITY

Is a bonafide work carried out by

ADARSH (4NM17CS008)

ASHWANTH V SHETTY (4NM17CS034)

In partial fulfilment of the requirements for the award of Bachelor of Engineering Degree in Computer Science and Engineering prescribed by Visvesvaraya Technological University, Belgaum during academic year 2019-2020.

It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report.

The mini project has been approved as it satisfies the academic requirements in respect of the work prescribed for the Bachelor of Engineering Degree.

Signature of Guide Signature of HOD

# **ACKNOWLEDGEMENT**

We believe that our project will be complete only after we thank the people who have contributed to make this project successful.

First and foremost, our sincere thanks to our beloved principal, **Dr. Niranjan N. Chiplunkar** for giving us an opportunity to carry out our project work at our college and providing us with all the needed facilities

.

We express our deep sense of gratitude and indebtedness to our guide **Mr.Radhakrishna Dodmane**, Associate Professor, Department of Computer Science and Engineering, for his inspiring guidance, constant encouragement, support and suggestions for improvement during the course of our project.

We sincerely thank **Dr. K.R. Udaya Kumar Reddy**, Head of Department of Computer Science and Engineering, Nitte Mahalinga Adyantaya Memorial Institute of Technology, Nitte.

We also thank all those who have supported us throughout the entire duration of our project.

Finally, we thank the staff members of the Department of Computer Science and Engineering and all our friends for their honest opinions and suggestions throughout the course of our project.

ADARSH (4NM17CS008)

ASHWANTH V SHETTY (4NM17CS034)

**ABSTRACT**

This project is aimed at studying the DES (Data Encryption Standard) and make necessary modifications to gain increased immunity to the attacks. From the study it has been observed that the DES is weak against the Linear Cryptanalytic Attack. Hence, this project is aimed to encrypt data in Non Linear Feedback shift style in circular fashion and to minimize the Linear Cryptanalytic Attack.

In this project we are also modifying the shared key using the plain text which is being encrypted. Since, we are encrypting 128 bytes of data the first 64 bits is used to generate the number –i.e The first key and first 64 bits of plain text is XOR’ed and then it is divided by 8 and the remainder obtained is used as the index where each key is complimented at that index.

Feistel structure and the key generation for each round, algorithm remains same as in normal DES implementation.

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| **TITLE** | **PAGE No.** |
| INTRODUCTION | 6 |
| LITRATURE SURVEY | 7-11 |
| PROBLEM DEFINATION | 12 |
| METHODOLOGY | 13-14 |
| ADVANTAGES & DISADVANTAGES | 15 |
| RESULT & DISCUSSION | 16-18 |
| CONCLUSION | 19 |

**CHAPTER 1**

**INTRODUCTION**

The success of E-commerce and m-commerce transactions depends on how transactions are carried out in the most secured manner. The prime requirements for any e-commerce and m-commerce transactions are Privacy, Authentication, Integrity maintenance and Non-Repudiation. Cryptography helps us in achieving these prime requirements. Today, various cryptographic algorithms have been developed.

The Data Encryption Standard (DES) was jointly developed in 1974 by IBM and the U.S. government (US patent 3,962,539) to set a standard that everyone could use to securely communicate with each other. It operates on blocks of 64 bits using a secret key that is 56 bits long. The original proposal used a secret key that was 64 bits long. It is widely believed that the removal of these 8 bits from the key was done to make it possible for U.S. government agencies to secretly crack messages

In this project we use both basic mathematics and also substitution method for both encrypting and decrypting process. The algorithm is modified to increase the security also for faster encryption.

**CHAPTER 2**

**LITRATURE SURVEY**

**DATA ENCRYPTION ALGORITHM :**

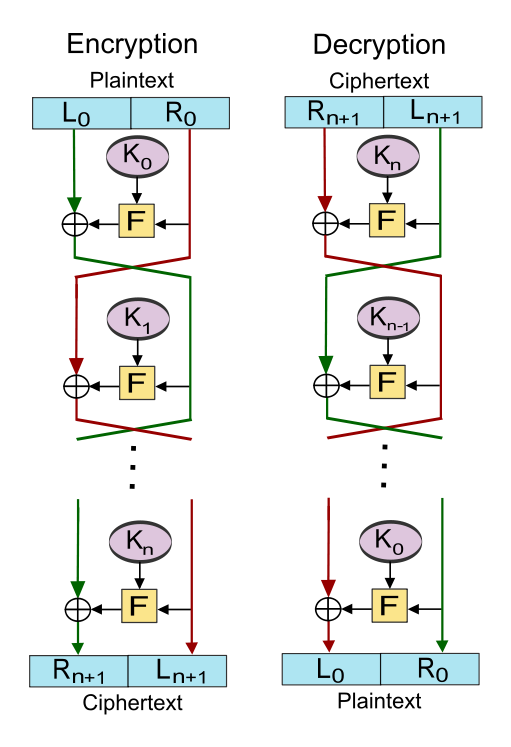
Introduction The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key1. Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP-1. The key-dependent computation can be simply defined in terms of a function f, called the cipher function, and a function KS called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function f is given in terms of primitive functions which are called the selection functions Si and the permutation function P. Si, P and KS of the algorithm

Feistel Cipher is not a specific scheme of a block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on a Feistel cipher structure uses the same algorithm for both encryption and decryption.

**ENCRYPTION PROCESS :**

Feistel Cipher is not a specific scheme of a block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on a Feistel cipher structure uses the same algorithm for both encryption and decryption.

Feistel Structure is shown in following illustration-



Encryption :

* The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
* In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function ‘f’ that takes two inputs − the key K and R. The function produces the output f(R, K). Then, we XOR the output of the mathematical function with L.
* In the real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
* The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round is the output L of the current round.
* Above substitution and permutation steps form a ‘round’. The number of rounds is specified by the algorithm design.
* Once the last round is completed then the two sub-blocks, ‘R’ and ‘L’ are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is a selection of round function ‘f’. To be an unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion

Decryption :

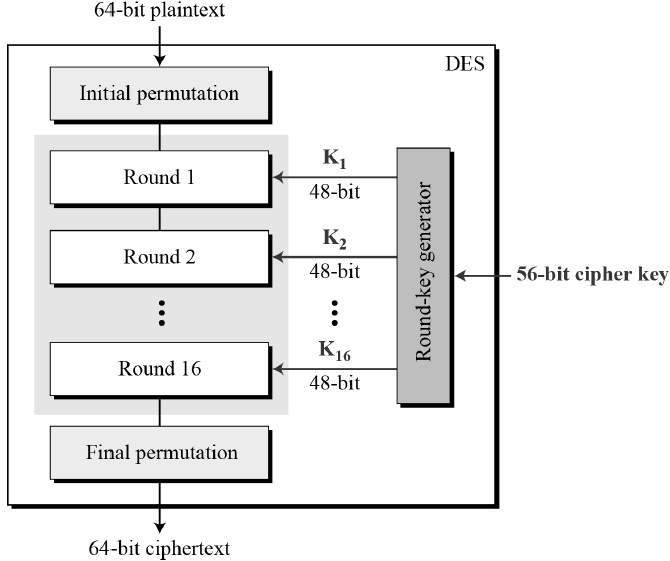
The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

The process is said to be almost similar and not exactly the same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of ‘L’ and ‘R’ in the last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

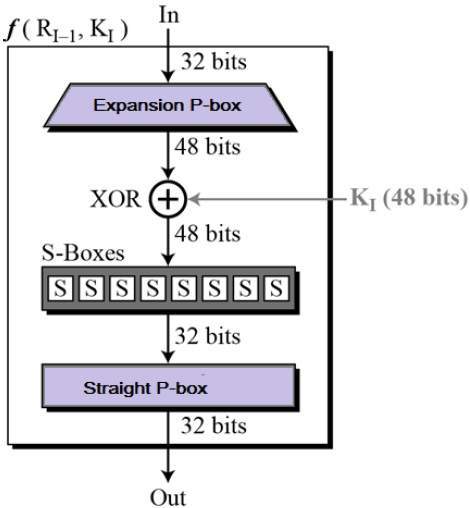
Number of Rounds :

The number of rounds used in a Feistel Cipher depends on desired security from the system. More rounds provide a more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. The number of rounds in the systems thus depends upon efficiency–security tradeoff.



Round function :

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



Weaknesses observed in DES algorithm :

Insecure due to the **keyspace size** i.e 56bits which is small compared to several other cryptographic algorithms. Cryptographic attacks are possible by mere **brute force** attacks. Not only that DES is a very well known algorithm hence the attacker might have the knowledge of algorithms making it easy to decipher.

**Chapter 3**

**Problem Defination**

The improvement proposed attempts to solve the problems by implementing the couple of approaches.

Encrypt 128 bytes of data in Non Linear Feedback shift style in circular fashion using different keys for each 8 bytes and to minimize the Linear Cryptanalytic Attack.

Modify the shared key using the plain text which is being encrypted. Since, we are encrypting 128 bytes of data the first 64 bits is used to generate the number –i.e. The first key and first 64 bits of plain text is XOR’ed and then it is divided by 8 and the remainder obtained is used as the index where each key is complimented at that index.

Feistel structure and the key generation for each round, algorithm remains same as in normal DES implementation.

**Chapter 4**

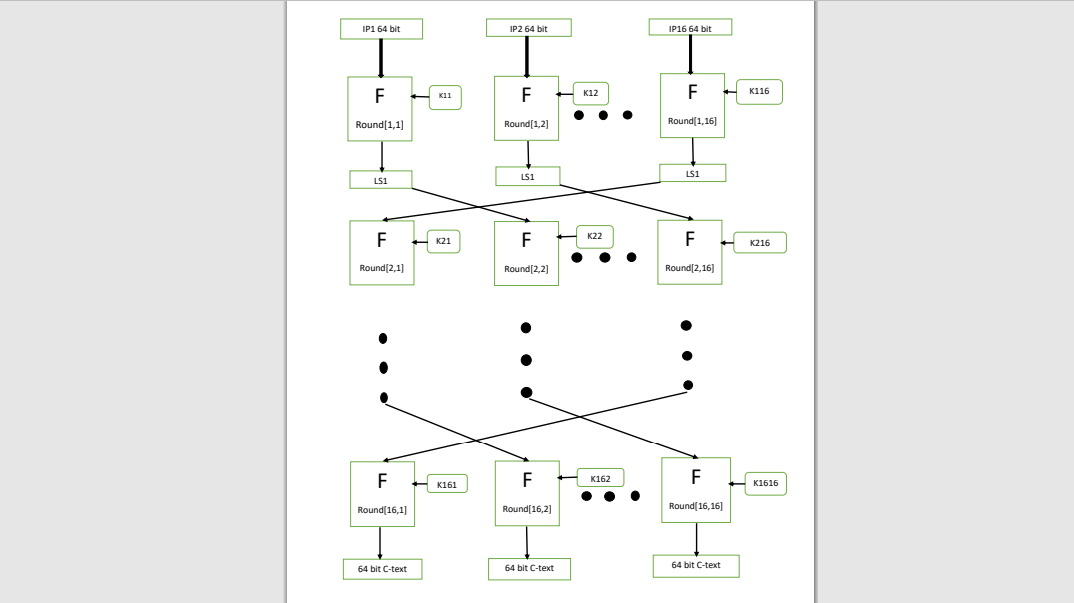
**Methodology**

Working of the improved DES :

The plaintext is divided into 64 bits and unlike in DES which encrypts data serially here 16 such blocks are encrypted parallelly using 16 different keys.

Here after each feistel round in each 64 bits of block that is being encrypted is left shifted and then it is passed to the next round of the encryption process which is using different key for encryption and is running prallelly along with this. The process is same for all 16 encrypting processes but, for output of each round of the 16th process is given to the first encryption process i.e in a circular fashion.

Diagram to illustrate the process of encryption :



Key modification based on input :

The shared key is also modified using the plain text which is being encrypted. Since, we are encrypting 128 bytes of data the first 64 bits is used to generate the number –i.e. The first key and first 64 bits of plain text is XOR’ed and then it is divided by 8 and the remainder obtained is used as the index where each key is complimented at that index.

Decryption :

The process of decryption remains same as encryption only having input as cipher text and the key modifier to modify the keys at the index whose value is the value of the key modifier which is being sent by the encryptor along with the cipher text, but after each round instead of left shifting right shifting is done.

**Chapter 5**

**Advantages, Disadvantages and Applications**

Advantages :

* Larger amount of data is encrypted using different keys.
* Security is increased.
* There is Non-Linearity in the generated cipher text.
* Better frequency distribution in cipher text.
* Lesser threat from cryptanalytic attack.
* Higher entropy than normal DES. (Regular DES entropy 7.96, modified DES entropy 7.99 of 8)

Disadvantages :

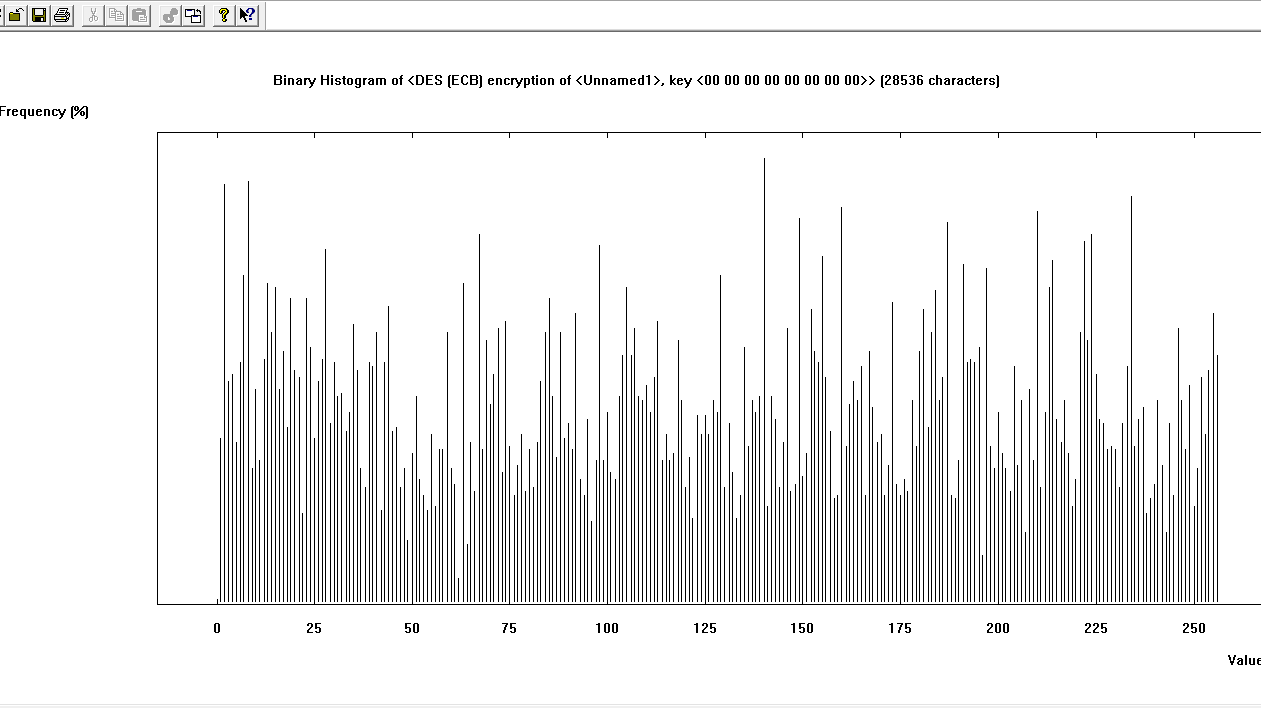
* The algorithm uses same key space hence, cryptographic attacks are possible as mere **brute force attacks**.
* The Standard DES algorithm is widely known and learnt hence, the chances of it getting attacked is more.
* The designed algorithm is comparatively slow to the normal DES. (Execution time for regular DES is 22.483 seconds and for modified DES it is 24.00 seconds)

**Chapter 6**

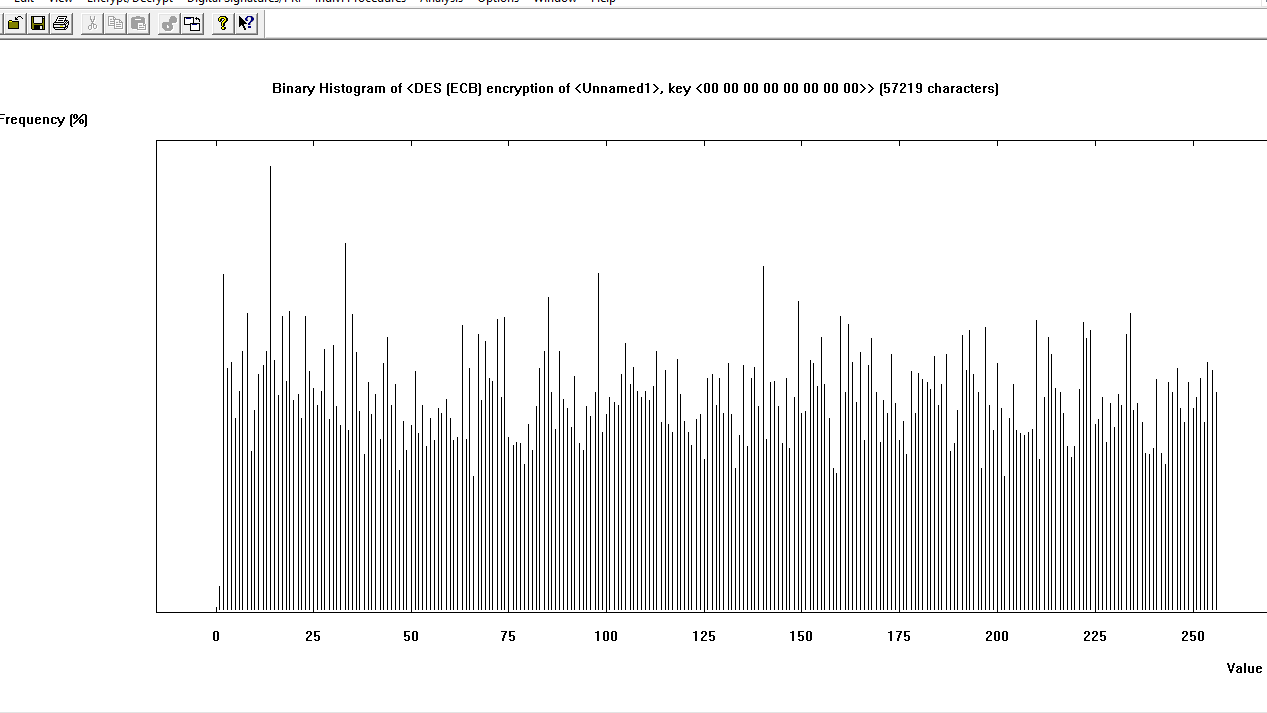
**Result and Discussion**

Since in this project we are encrypting the image the size of the photo string and as well as the encrypted message is too long to be contained in this Report but, they are uploaded to the GitHub Repository whose link is provided in the Reference section (Chapter 7) and also it is zipped along with this Report.

Histogram comparison between Cipher text of normal DES and modified DES :



DES Cipher text (values ranging from 0 – 255)

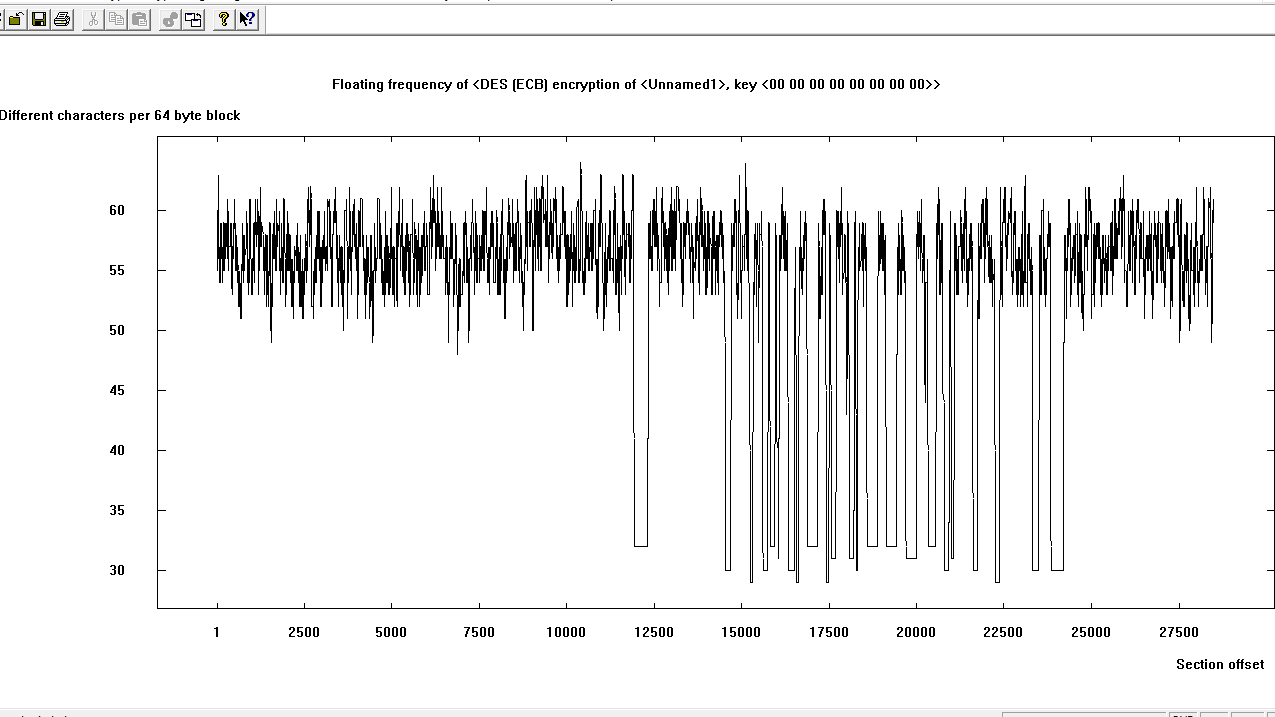


Modified DES Cipher text (values ranging from 0 – 255)

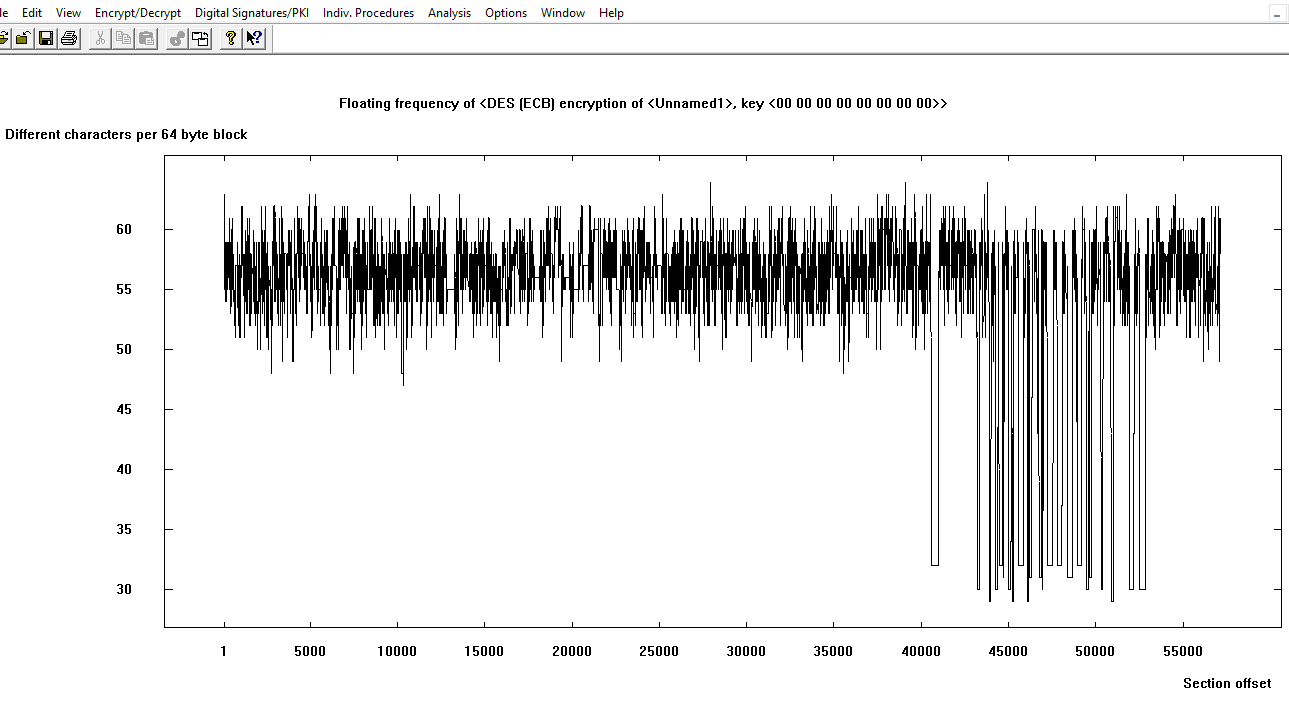
Entropy :

* Normal DES Cipher text : 7.96 of 8
* Modified DES Cipher text : 7.99 of 8

Floating Frequency Comparison :



DES Cipher text



Modified DES Cipher text

Result :

From the above criteria’s we can say that the Modified DES has more Security than the Normal DES.

**CHAPTER 7**

**Reference**

* Code for regular DES : <https://github.com/RobinDavid/pydes> (reference code which was modified.
* Code for modified DES : <https://github.com/Adarsh999bh/des> ( modified to obtain the advantages specified in the Chapter 5)