NITTE MAHALINGA ADYANTHAYA MEMORIAL INSTITUTE OF TECHNOLOGY

An Autonomous College Affiliated to VTU Belgaum
Nitte -574110, Udupi District

PROJECT REPORT

ON

Enhancement of SDES to process large integer using RNS

Submitted by

Brian Steve Pinto
4nm17cs045
6th Sem A Section
Dept. Of CSE

Brian Stevo Aranha
4nm17cs046
6th Sem A Section
Dept. of CSE

Submitted to

Mr. Radhakrishna Dodmane
Associate Professor
Dept. Of CSE
NMAM Institute of Technology

NMAM INSTITUTE OF TECHNOLOGY
(An autonomous Institute affiliated to VTU, Belgaum)
Nitte-574110, Karkala, Udupi District
Department of Computer Science and Engineering

CERTIFICATE

Certified that the project work carried out by Brian Stevo Aranha, USN 4NM17CS046 and Brian Steve Pinto, USN 4NM17CS045, bonafide students of NMAM Institute of Technology, Nitte in fulfilment for the Subject Cryptography and Network Security in Computer Science and Engineering during the academic year 2019 – 2020.

Signature of lecturer

Date:

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible because
“Success is the abstract of hard work and perseverance, but steadfast of all is encouraging guidance.”
So, We acknowledge all those whose guidance and encouragement served as a beacon light and crowned our efforts with success.
I would like to thank our principal Prof. Niranjan N. Chiplunkar firstly, for providing us with this unique opportunity to do the project in the 6th semester of Computer Science and engineering.
I would like to thank our college administration for providing a conductive environment and also suitable facilities for this project.
I would like to thank our HOD Prof.Uday Kumar Reddy for showing us the path and providing the inspiration required for taking the project to its completion. It is my great pleasure to thank our guide Mr. Radhakrishna Dodmane for his continuous encouragement, guidance and support throughout this project.
We thank all the staff members of the department of CSE for providing resources for the completion of the project.

BRIAN STEVO ARANHA
(4NM17CS046)
BRIAN STEVE PINTO
(4NM17CS045)

Abstract

Enhanced Simplified Data Encryption Standard Algorithm to protect data and to provide Security to the data.ESDES Algorithm uses number of operations and rounds applied to blocks. It computes complement operation when text is converted from ASCII to binary. Large Number is Decomposed to achieve parallel processing of bits. Adding 1's complement operations gives additional security and making it difficult for the intruder to attack. As the complexity is increased the encryption and decryption time is also increased.

Objective

- Reducing the Complexity of Large number
- To create in built parallelism between the numbers using Decomposition
- Minimize the side channel attacks

INDEX

<u>**INTRODUCTION of SDES**</u>

SDES Key Generation

SDES uses 10-bit key shared between sender and Receiver. From this key, two 8-bit sub-keys are generated .Let the 10-bit key be represented as {B1 B2 B3 B4 B5 B6 B7 B8 B9 B10}. Now permutation P10 is applied on the 10-bit key, and is represented as {B3 B5 B2 B7 B4 B10 B1 B9 B8 B6}, denoted by X. Now X is divided into two parts, the left 5 bits are X1and right 5 bits are X2. Thus X1={B3 B5 B2 B7 B4}, and X2={B10 B1 B9 B8 B6}. Now apply circular shift left operation on X1and X2separately. Such that X1= {B5 B2 B7 B4 B3}, X2 = {B1 B9 B8 B6 B10}. After left shift operation, combine the results of X1 and X2 and denote as Y. And then apply permutation P8 to Y, then it becomes {B1 B7 B9 B4 B8 B10 B3 B6} which is key K1and again apply left shift operation to the X1 and X2,it is represented as {B2 B7 B4 B10 B1 B9 B8 B6 B3 B5}which is Z. And again apply P8 to the Z. So the result is K2. K1and K2 are utilized for encryption and decryption

SDES Encryption

The plaintext is divided into 8-bit blocks and encryption process is applied. Let the 8-bit plaintext be represented as {b1 b2 b3 b4 b5 b6 b7 b8}. Now initial permutation IP is applied on the 8-bit Plaintext,and is represented as {b2 b6 b3 b1 b4 b8 b5 b7},denoted by A. Now A is divided into two parts, the left 4 bits are A1and right 4 bits are A2. Thus A1={b2 b6 b3 b1}, and A2={b4 b8 b5 b7}. Now we apply Function fk.In this function we apply Expansion/Permutation (E/P). Now apply Expansion/Permutation (E/P) to A2, then it becomes {b7 b4 b8 b5 b8 b5 b7 b4} denoted as B. Now we apply XOR operation with K1and B is denoted as C. Now, C is divided into two parts, the left 4 bits are C1and right 4 bits are C2. Now C1, C2put into S-Boxes. Here S-boxes is nothing but replacing a bit with another bit.

$$S_0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S_1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

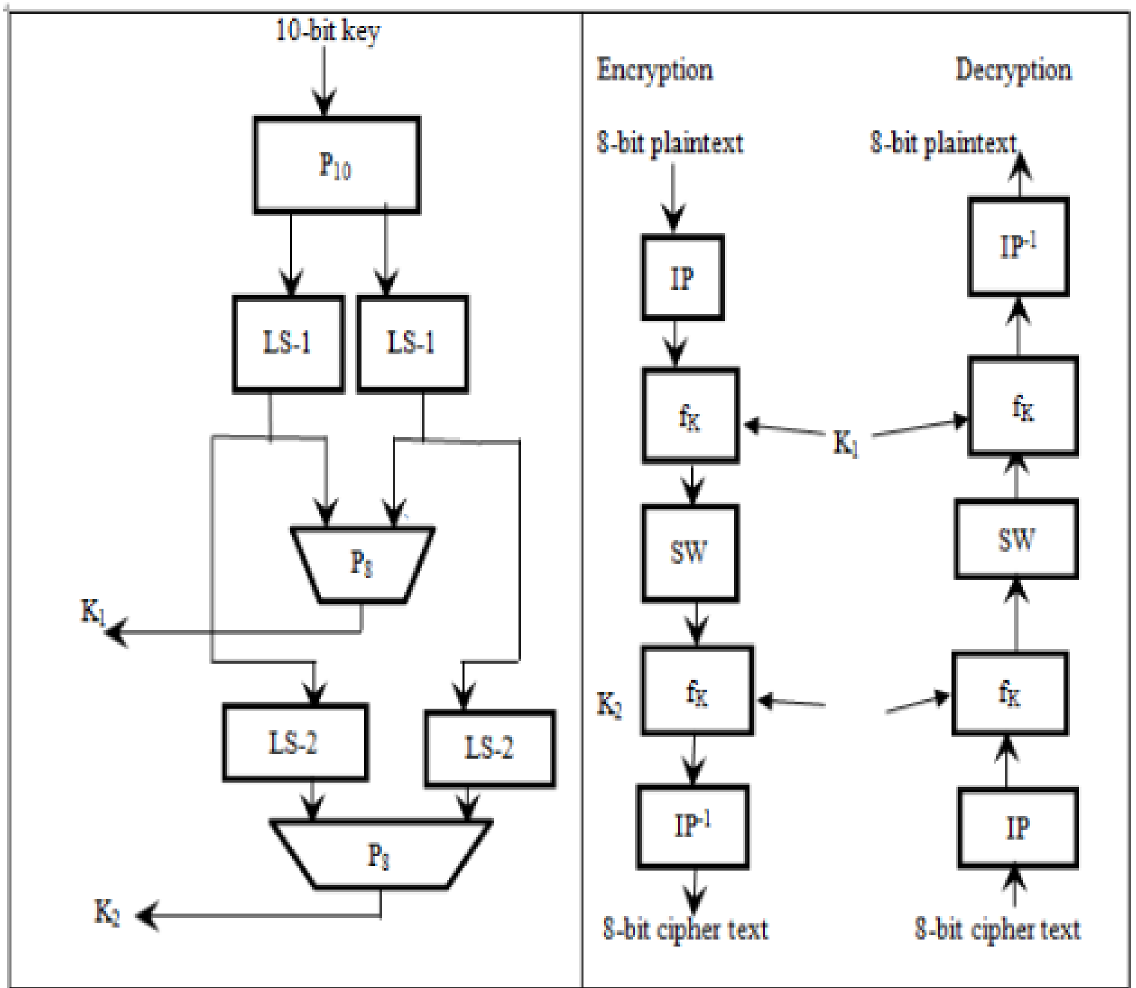


Fig.1. Key generation of SDES

Fig.2. Simplified DES Scheme

For C1, S-Box is called S0 and for C2, S-Boxis called S1. For S0,consider C1(b1 b4) as row and C1(b2 b3) as column. For S1, consider C2(b5 b8) as row and C2(b6 b7) as column.So,we get result and it is represented as(b1 b2 b3 b4)denoted as D. apply P4 to the D so the result is(b2 b4 b3 b1)is denoted as E. Now perform XOR operation for Eand A1and we get the result as (b1 b2 b3 b4) is denoted as F. So we consider F as left half and A2as right half. Switch(SW) the parts we get the result as (b1 b2 b3 b4 b5 b6 b7 b8) is denoted as G. so again it is divided to two parts left as G1and right as G2. And again apply Expansion/Permutation (E/P)for G2 is denoted as H. Perform XOR operation to H with K2 is denoted as I. So, the result I is divided to two parts left as I1 and right as I2.Now I1,I2put into S-Boxes. Put I1 intoS-Box S0and I2 into S-Box S1. For S0,consider I1(b1 b4) as row and I1(b2 b3) as column. For S1, consider I2(b5 b8) gas row and I2(b6 b7) as column. So,We get result and it is represented as (b1 b2 b3 b4)denoted by J.apply P4(b1 b2 b3 b4)to the J then the result is(b2 b4 b3 b1)is denoted as K. Now perform XOR operation for K and G1 denoted as L. Now consider L as the left half and G1 as the right half and we get it as b1 {b2 b3 b4 b5 b6 b7 b8} denoted as M. Now apply permutation IP-1to the M, the result is {b4 b1 b3 b5 b7 b2 b8 b6 } is denoted as N which is the final result.

SDES Decryption

The decryption algprithm is similar to encryption and reverse of encryption. Decryption process is required to make sure that the SDES algorithm can decipher the ciphertext back to its original form and the input and output for decryption is shown in Fig2. With a 10-bit key, there are just 210 bpossibilities. So brute force attack can be done to find the plain text. For avoiding this drawback we are introducing improved SDES algorithm in which for every block shift operations differ, hence possibilities of finding key and also knowing plaintext becomes difficult. Attacker cannot find the plaintext

Modification of SDES

ESDES Key Generation

Permutation P10 is applied on the 10-bit key. Then the key is complemented (x). The complemented key is divided into two parts (x1 and x2) . Apply circular left shift operation. Combine the result and apply P8 which gives KEY 1. Combined result of leftshift operation (x1 and x2) is complemented . Then divided into two parts . Perform left shift operation twice. Combine the result and apply P8 which gives KEY 2. KEY1 and KEY2 are utilized for encryption and decryption.

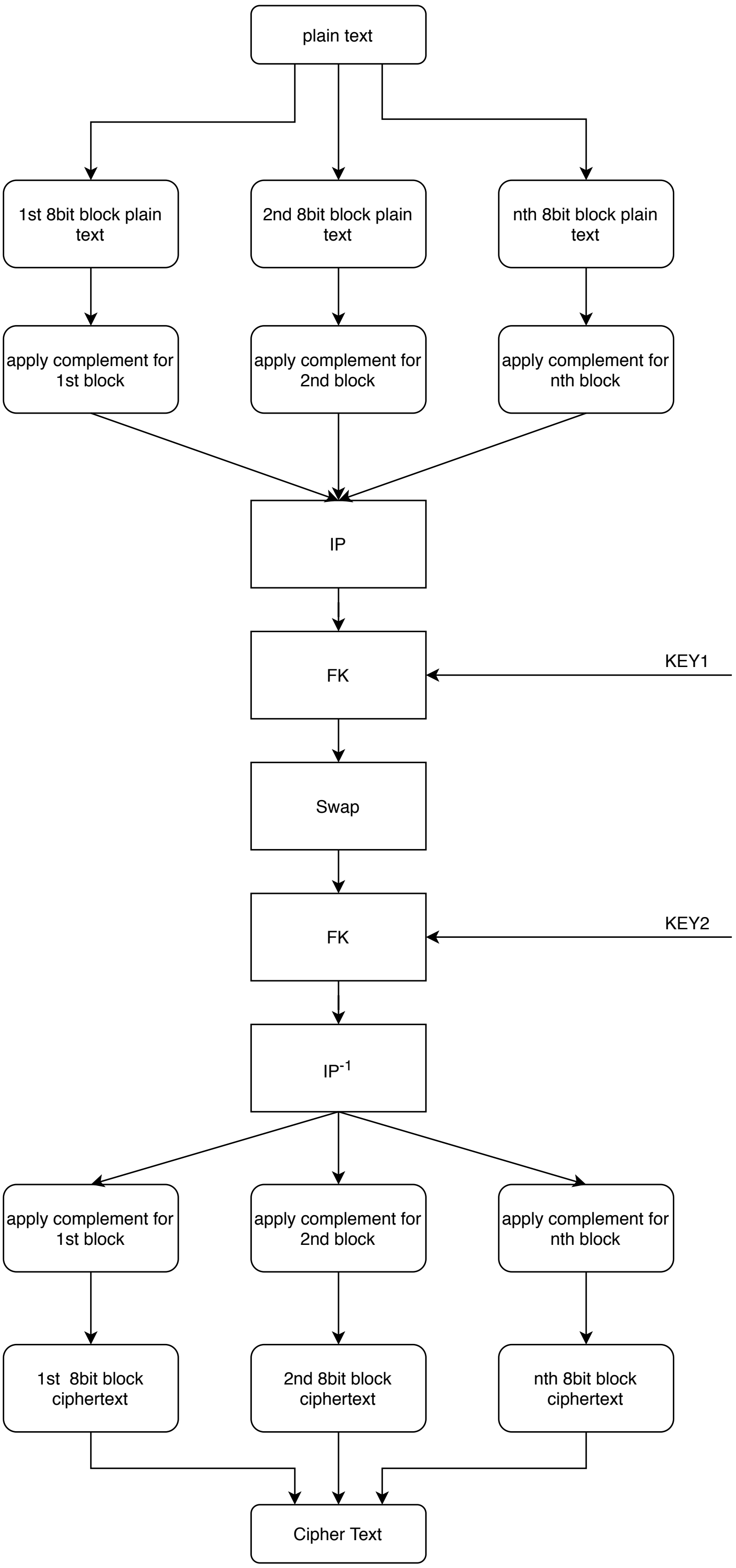
ESDES Encryption

Plaintext is converted into ASCII and then to binary. Binary text is divided into blocks of 8-bits. Then apply complement for each block of bits. The generated 8-bit text is encrypted based on SDES and is complemented after IP inverse.
8-bit block plain text is complemented. Initial permutation is performed on complemented plain text (denoted by A).Now A is divided into two parts (A1 And A2). Apply Function Fk. In this Function we apply Expansion/Permutation (E/P) to right half of A that is A2. Next we apply XOR operation with KEY1 and is divided into two parts,the left 4-bits are B1 and right 4-bits are B2. Next B1 and B2 are put into S-Boxes. Apply P4 on the obtained result. Perform XOR on the obtained result with A1(left side of A). Consider the result as left half and A2 as right half. Swap the left and right side. Apply Function Fk on the obtained result (again). Perform IP inverse on the final result of FK. Complement the obtained result. The result obtained is the final Ciphertext for the 8-bit block plain text.

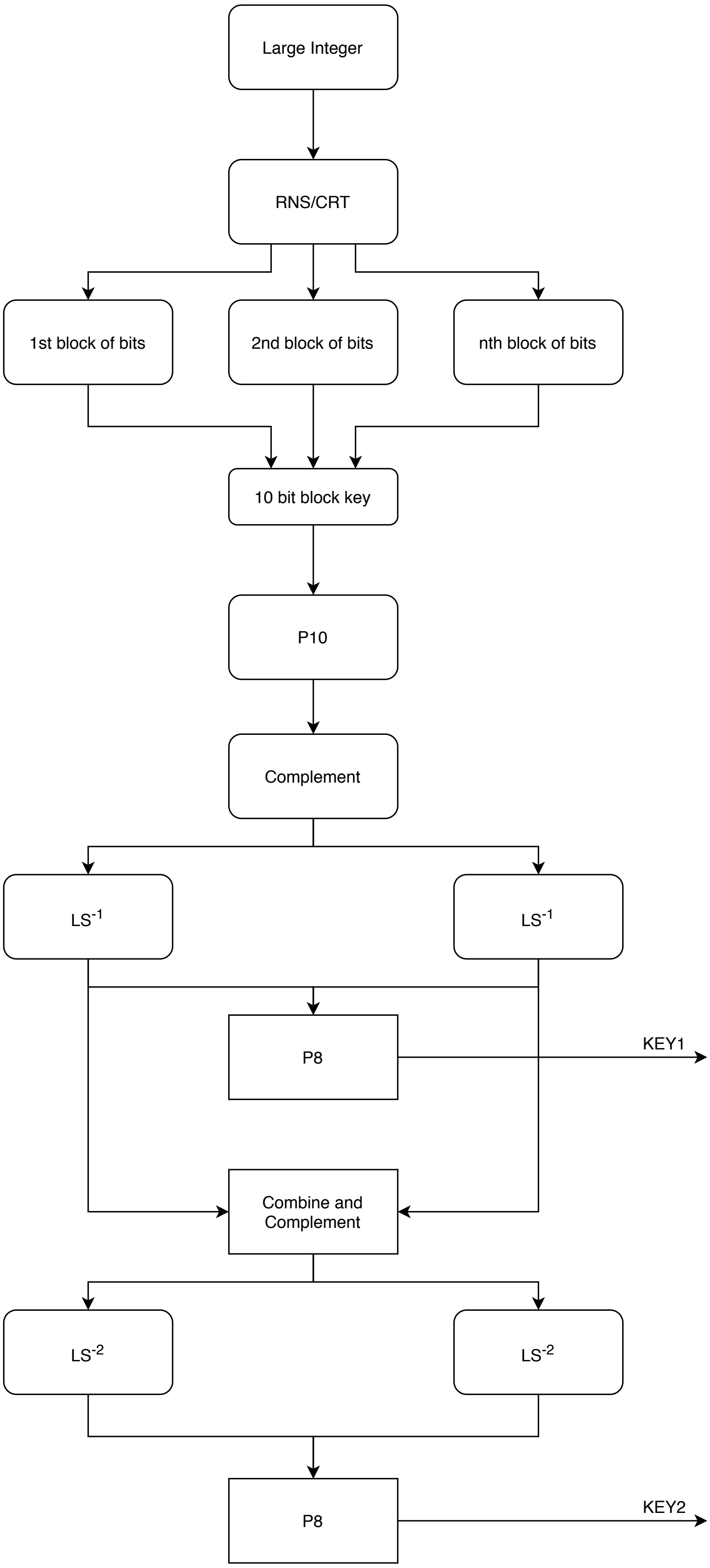
ESDES Decryption

Decryption is the reverse of encryption.cipher text is divided into blocks. Each block contains 8-bits.then we complement the bits and the reverse of encryption is applied and we get the plain text.

ESDES ENCRYPTION



KEY GENERATION



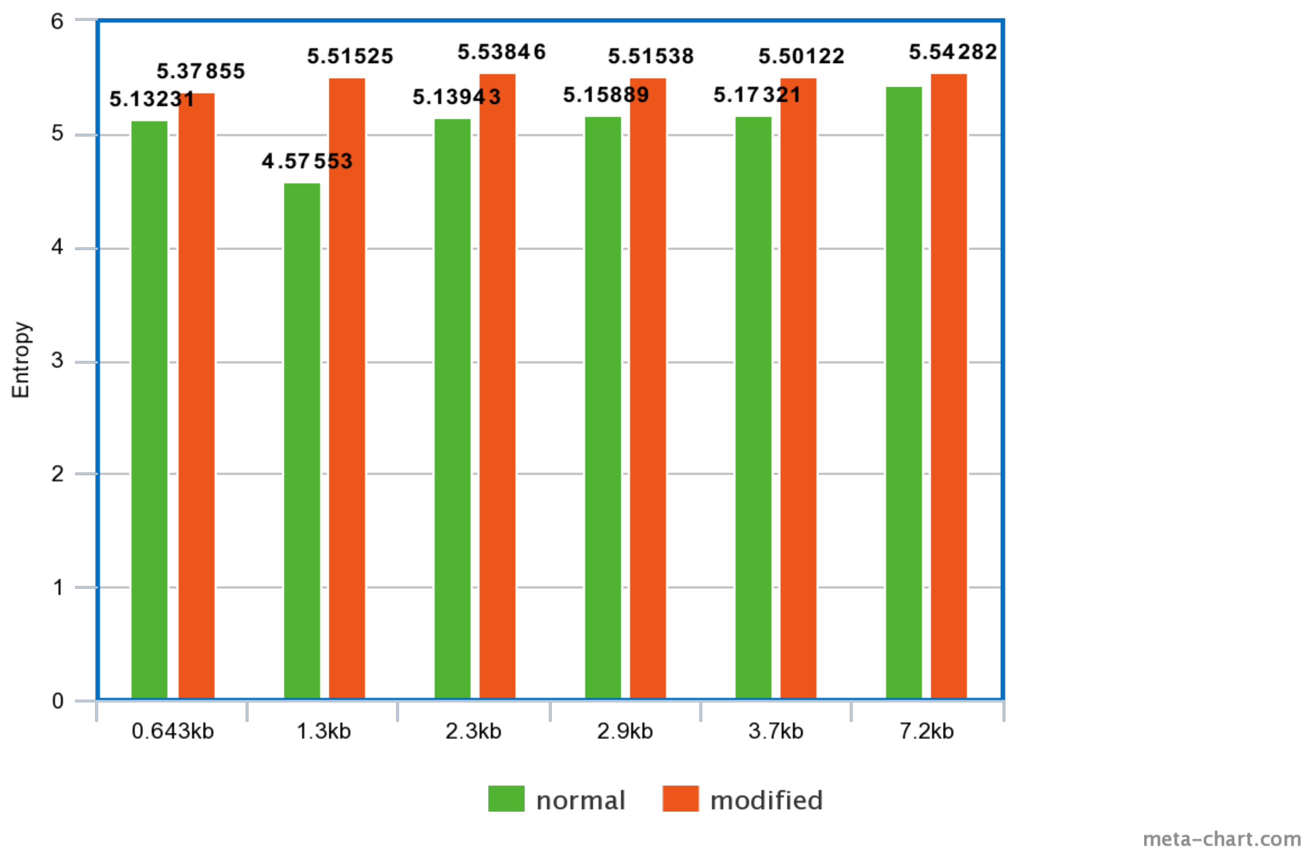
RESULT

Entropy values:

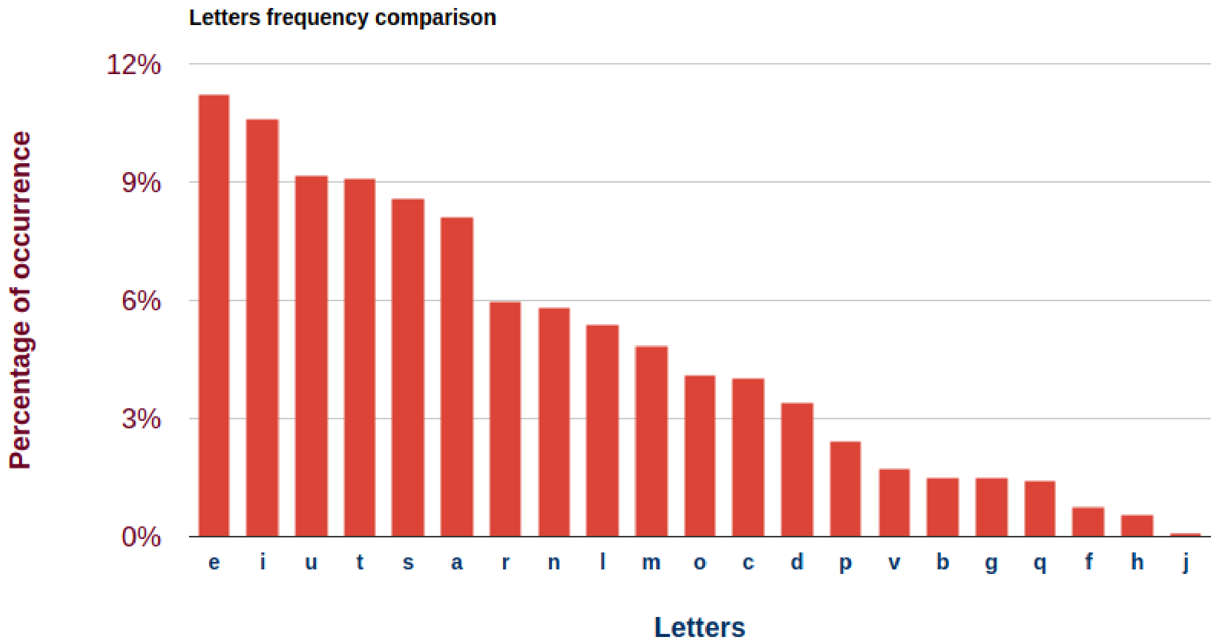
FILE SIZE	PLAINTEXT	CIPHERTEXT (SDES)	CIPHERTEXT (ESDES)
0.643kb	4.39563	5.13231	5.37855
1.3kb	4.40201	4.57553	5.51525
2.3kb	4.38599	5.13934	5.53846
2.9kb	4.41865	5.15889	5.51538
3.7kb	4.38599	5.17321	5.50122
7.2kb	4.20667	5.42854	5.54282

ENTROPY is a measure of unpredictability of information contained in the message. In simple terms, higher entropy in messages makes it difficult for the cryptanalyst to get the plain text back, assuming that the cipher text is known.
The graph depicts the entropy value for files of different size.

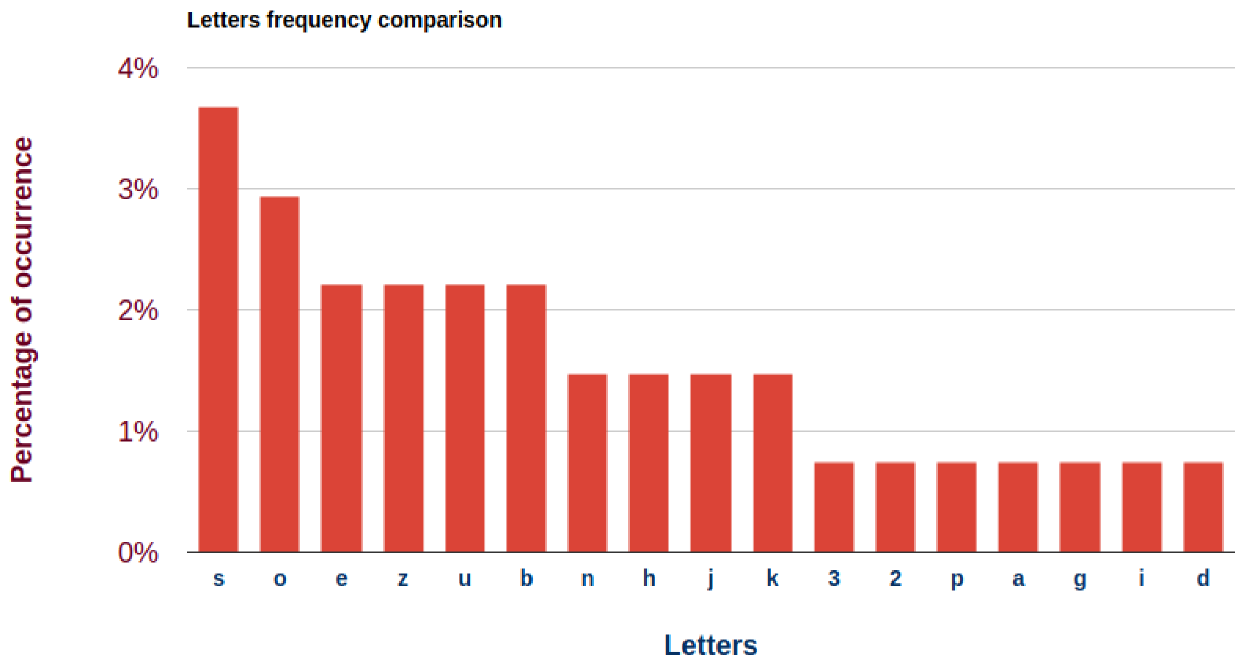
GRAPH FOR ENTROPY:



HISTOGRAM FOR PLAINTEXT:



HISTOGRAM FOR CIPHERTEXT(Alphabet):



HISTOGRAM FOR CIPHERTEXT(special characters):