МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра программной инженерии

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программное обеспечение информационных технологий (программирование интернет-приложений)

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ:

по дисциплине «Информационная безопасность»

Исполнитель

студент (ка) 3 курса группы 6 Розель Станислав Александрович

(Ф.И.О.)

Минск 2025

1. **DES**

В ходе лабораторной работы нужно было реализовать алгоритм шифрования DES. Реализация раундов в DES представлен в листинге 1.1

|  |
| --- |
| desRound(block, subkey) {  let left = block.slice(0, 32);  let right = block.slice(32);  const fResult = this.f(right, subkey);  const xored = this.xor(left, fResult);  return [right, xored];  } |

Листинг 1.1 – Раунд шифра DES

На листинге 1.2 представлена реализация f-функции:

|  |
| --- |
| f(right, subkey) {  const expanded = this.permute(right, this.E);  const xored = this.xor(expanded, subkey);  const sBoxesOutput = [];  for (let i = 0; i < 8; i++) {  const block = xored.slice(i \* 6, (i + 1) \* 6);  const row = this.bitsToNumber([block[0], block[5]]);  const col = this.bitsToNumber(block.slice(1, 5));  const sValue = this.S[i][row][col];  sBoxesOutput.push(...this.numberToBits(sValue, 4));  }  return this.permute(sBoxesOutput, this.P);  } |

Листинг 1.2 – F – функция

Так же в ходе лабораторной работы было измерено время для шифрования и расшифрования, которое составило 23.65ms и 11.65ms соответственно.

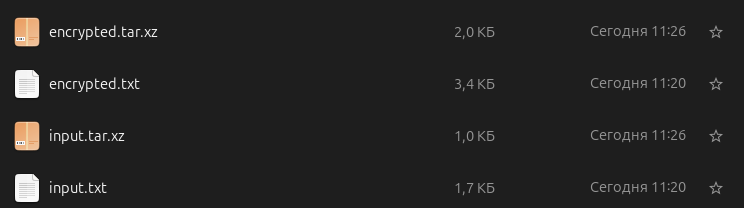
Сравнение размеров сжатых и оригинальных исходного и зашифрованного текстов представлено на рисунке 1.1. 

Рисунок 1.1 Сравнение размера