Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №7**

Исследование блочных шифров

Выполнил:

Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

2024

Для выполнения данной лабораторной работы была разработана программа на языке Python. Используемый алгоритм – DES-EEE3.

DES-EEE3: является усовершенствованной версией DES, которая использует три ключа для операций шифрования и расшифрования.

DES-EEE3 отличается от базового DES следующими основными аспектами:

Длина ключа: DES использует ключ длиной в 56 бит, тогда как DES-EEE3 использует три ключа длиной в 56 бит каждый, что в сумме составляет 168 бит. Благодаря использованию трех ключей DES-EEE3 обеспечивает более высокий уровень безопасности.

Количество раундов: DES выполняет 16 раундов шифрования на каждый блок данных, тогда как DES-EEE3 выполняет три операции шифрования/расшифрования с разными ключами. Каждая операция использует алгоритм DES, выполняющий 16 раундов. Таким образом, DES-EEE3 фактически выполняет 48 раундов шифрования/расшифрования на каждый блок данных

Было проанализировано влияние слабых и полуслабых ключей на конечный результат зашифрования и лавинный эффект. Для оценки лавинного эффекта был зашифрован текст с исходными ключами, затем были изменены 2 символа в ключе и произведено шифрования открытого текста заново.

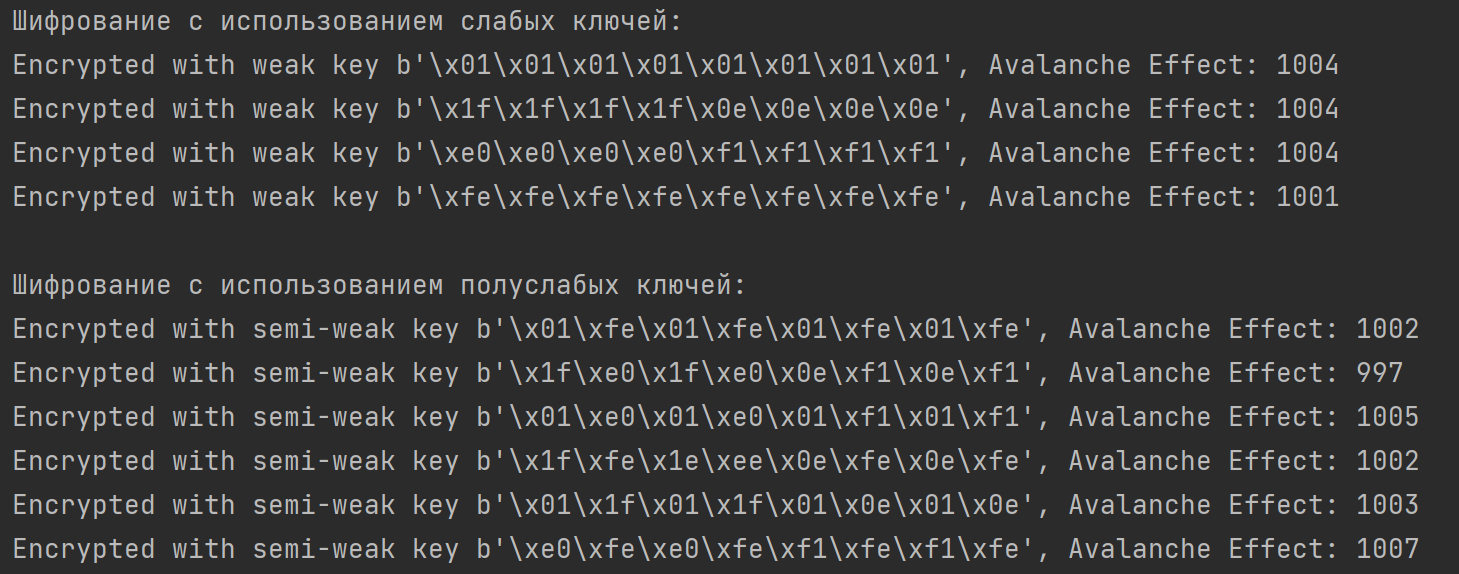


Рисунок 1 – Шифрование используя слабые, полуслабые ключи и их0020лавинный эффект

Для оценки степени сжатия использовались встроенные средства языка программирования python.

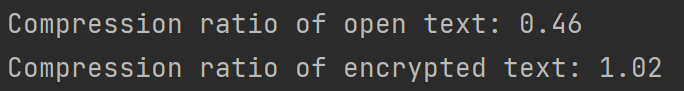


Рисунок 2 – Степень сжатия исходного и зашифрованного текста

Также было измерено время шифрования и расшифрования алгоритмом DES-EEE3.

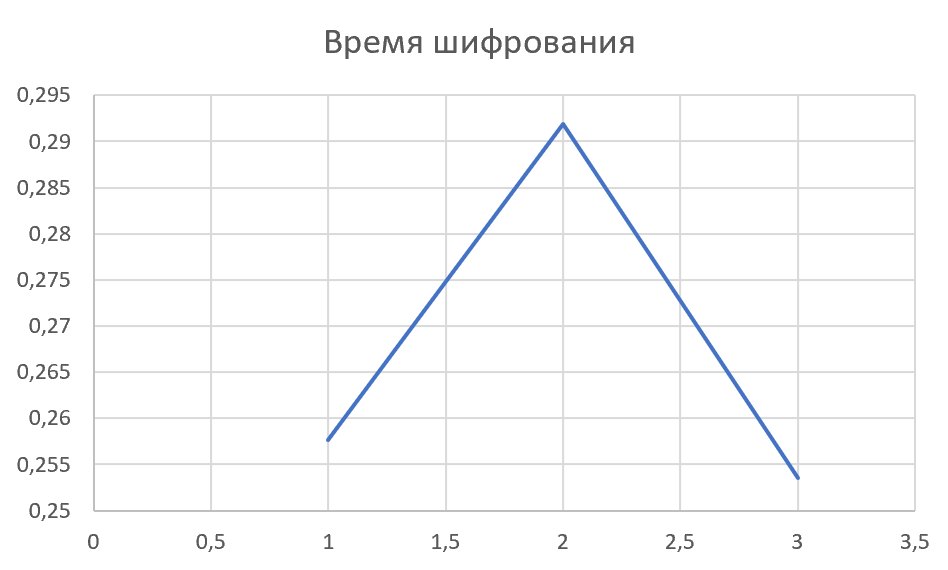


Рисунок 3 – Время шифрования алгоритмом DES-EEE3

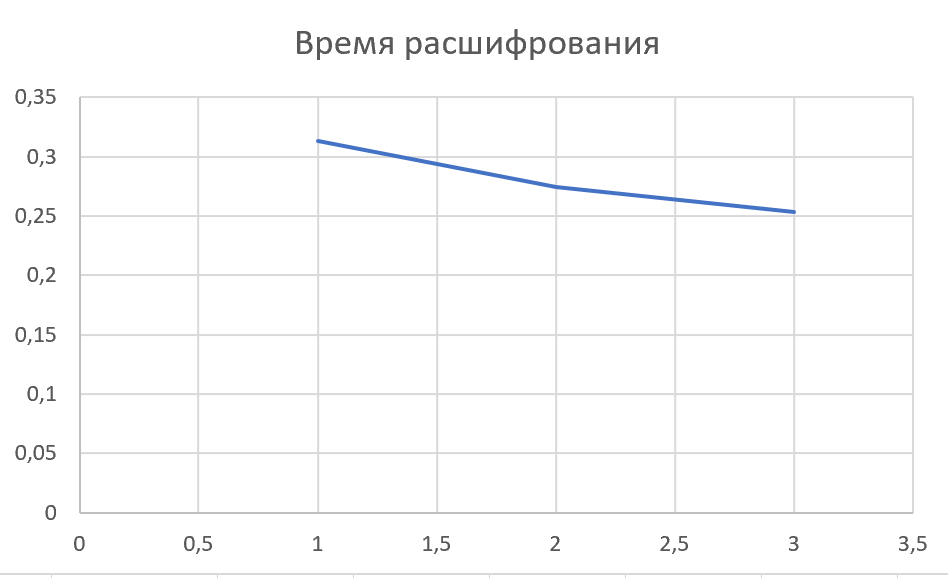


Рисунок 4 – Время расшифрования алгоритмом DES-EEE3

**Выводы:** DES-EEE3 обеспечивает более высокий уровень безопасности по сравнению с базовым DES за счет использования трех ключей и выполнения трех операций шифрования-расшифрования-шифрования.

DES-EEE3 требует больше вычислительных ресурсов и времени для шифрования и расшифрования данных, чем DES.