**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра информационной безопасности**

отчет

**по лабораторной работе №4**

**по дисциплине «Криптография и защита информации»**

Тема: Изучение шифра DES

|  |  |  |
| --- | --- | --- |
| Студент гр. 8383 |  | Киреев К.А. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

**Цель работы.**

Исследовать шифры DES, 3DES, а также другие модификации шифра DES: DESX, DESL, DESXL и получить практические навыки работы с ними, в том числе с использованием приложения Cryptool 1 и 2.

***Исследование преобразований DES***

1*.* Изучить преобразования шифра DES с помощью демонстрационного приложения из Cryptool 1.

Indiv.Procedures -> Visualization… -> DES…

В программе Cryptool 1 был запущен демонстрационный пример. Результат выполнения приведен на рис. 1

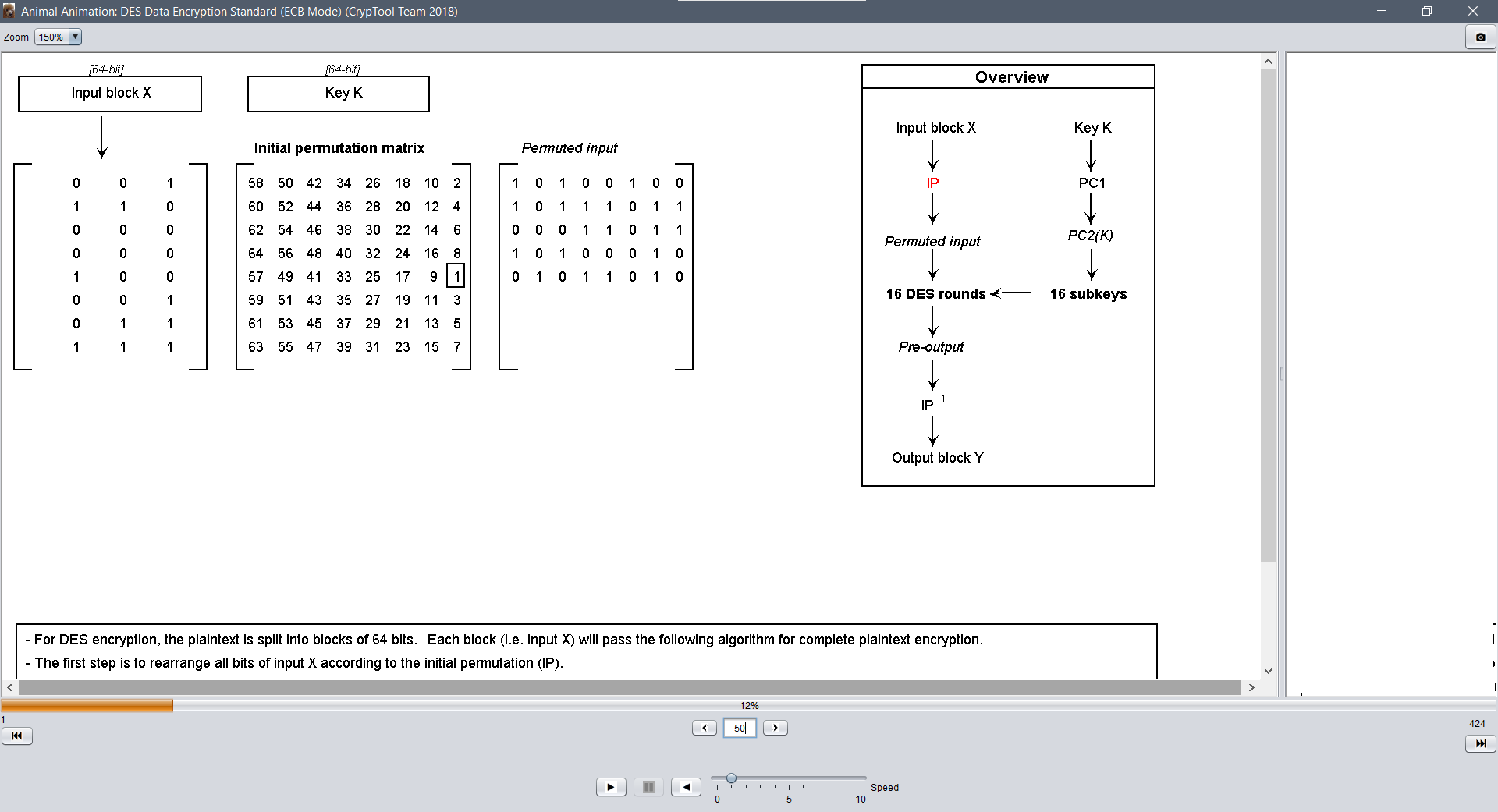


Рисунок 1 – Запуск демонстрационного примера

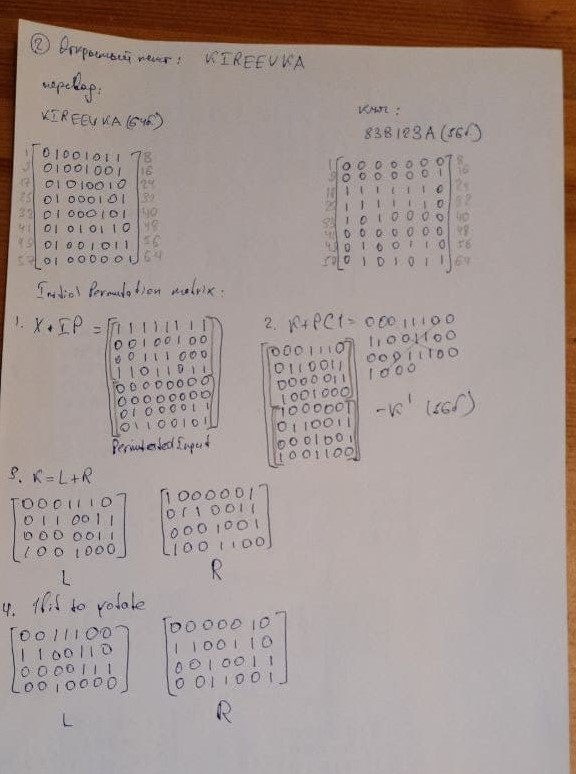
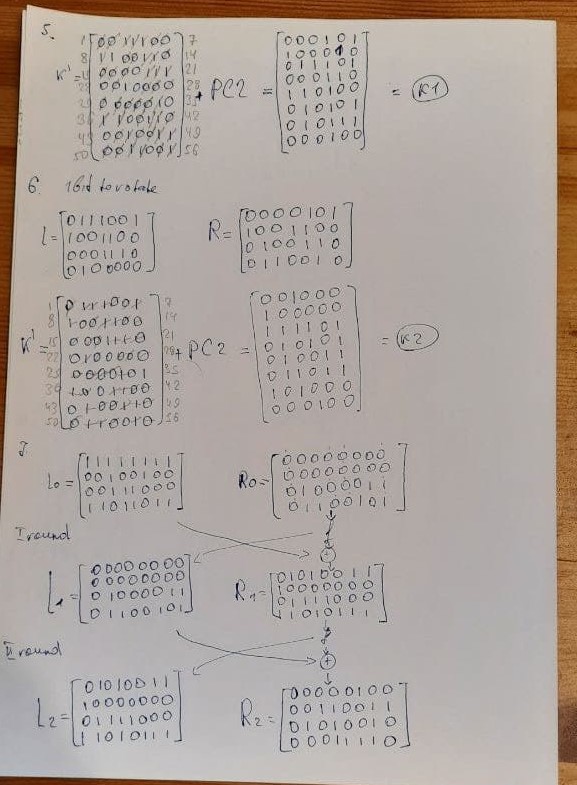
2. Выполнить вручную преобразования первых двух раундов и вычисление раундовых ключей при следующих исходных данных:

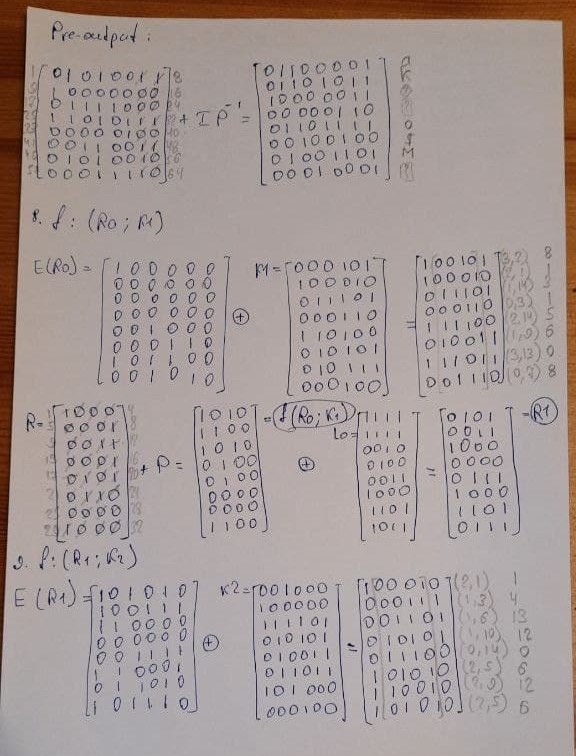
a. Открытый текст (не более 64 бит) – фамилия\_имя (транслитерация латиницей)

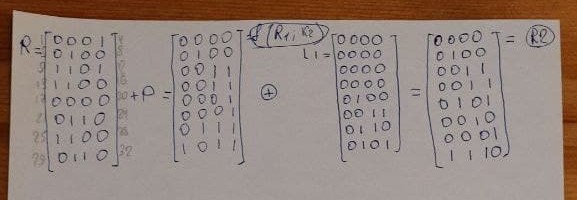
b. Ключ (56 бит) – номер зачетной книжки и инициал отчества (всего 7 символов)

3. Выполнить вручную обратное преобразование зашифрованного сообщения

4. Убедиться в совпадении результатов

На рис. 2 представлен результат выполнения 2 и 3 пунктов данного подпункта.

****

****

***Исследование DES в режимах ECB и CBC.***

*Основные параметры и обобщенная схема шифров.*

В режиме ECB шифра DES используется независимо для каждого 64-битного блока шифруемых данных. Схема использования шифра в режиме ECB представлена на рисунке.

В режиме CBC перед запуском DES для зашифрования каждого очередного блока открытого текста происходит побитовое XOR-сложение этого блока с блоком зашифрованного текста из предыдущего шага.

|  |  |
| --- | --- |
|  |  |
| ECB — Electronic Code Book | CBC — Cipher Block Chaining  IV – Initialization Vector |

1. Создать картинку со своими ФИО (формат bmp).

Картинка для шифрования была создана в приложении Paint и представлена на рис. 3.



Рисунок 3 – Картинка с ФИО

1. Зашифровать картинку шифром DES в режиме ECB.

Используя ключ ABCD, зашифруем в Cryprool картинку из первого пункта шифром DES в режиме ECB. Результат представлен на рис. 4

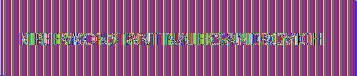


Рисунок 4 – Картинка, зашифрованная шифром DES в режиме ECB

1. Зашифровать картинку шифром DES в режиме CBC c тем же ключом.

Используя ключ ABCD, зашифруем в Cryprool картинку из первого пункта шифром DES в режиме CBC. Результат представлен на рис. 5



Рисунок 5 – Картинка, зашифрованная шифром DES в режиме CBC

1. Сохранить скриншоты картинок для отчета.

Картинки представлены в пунктах 2 и 3.

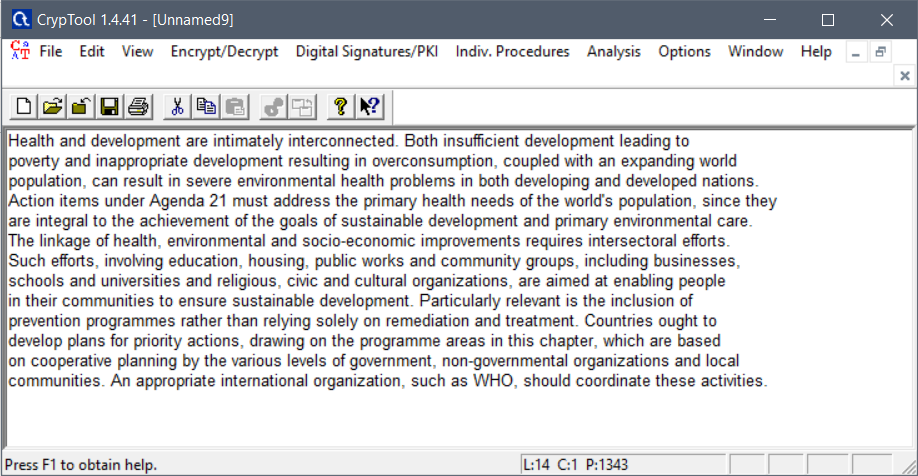
1. Сжать исходную и 2 зашифрованных картинки средствами CrypTool. Зафиксировать размеры полученных файлов в таблице.

*Таблица 1 – Размер сжатых файлов*

|  |  |  |
| --- | --- | --- |
|  | *Изначальный размер* | *Размер после сжатия* |
| *Исходная картинка* | 79.6 КБ | 1.17 КБ |
| *Картинка, зашифрованная шифром DES в режиме ECB* | 79.6 КБ | 3.36 КБ |
| *Картинка, зашифрованная шифром DES в режиме CBC* | 79.6 КБ | 79.6 КБ |

1. Выбрать случайный текст на английском языке (не менее 1000 знаков) и зашифровать его DES в режиме ECB.

Был выбран фрагмент текста English.txt.



1. Для одного и того же шифротекста оценить время проведения атаки «грубой силы» в случаях, когда известно байт секретного ключа. Зафиксировать результаты измерений в таблице.

Была проведена атака «грубой силы» в случаях, когда известна некоторая часть ключа. Результаты занесены в таблицу 2.

Таблица 2 – Зависимость времени расшифровки при известной части ключа (ECB)

|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 2 | 1.2 года |
| 3 | 6.2 дня |
| 4 | 59 минуты |
| 5 | 35 секунд |
| 6 | Около 1 секунды |
| 7 | < 1 секунды |

1. Повторить подобные измерения для DES в режиме CBC.

Была проведена атака «грубой силы» в случаях, когда известна некоторая часть ключа. Результаты занесены в таблицу 3.

Таблица 3 – Зависимость времени расшифровки при известной части ключа (CBC)

|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 2 | 2.8 года |
| 3 | 9.1 дня |
| 4 | 1.5 часа |
| 5 | 45 секунд |
| 6 | Около 1 секунды |
| 7 | < 1 секунды |

**Исследование 3-DES.**

*Основные параметры и обобщенная схема шифров.*

Шифр 3-DES состоит в трехкратном применении обычного DES. Существует 4 основные версии данного шифра:

1. DES-EEE3 – шифрование происходит 3 раза независимыми

ключами

2. DES-EDE3 – операции шифровка-расшифровка-шифровка с тремя разными ключами

3. DES-EEE2 – то же что и DES-EEE3, но на первом и последнем шаге одинаковый ключ

4. DES-EDE2 – то же что и DES-EDE3, но на первом и последнем шаге используется один и тот же ключ

На текущий момент самыми популярными версиями шифра являются DES-EDE3 и DES-EDE2.

1. Выбрать случайный текст на английском языке (не менее 1000 знаков).

Был выбран тот же текст, что и в пункте 2.6.

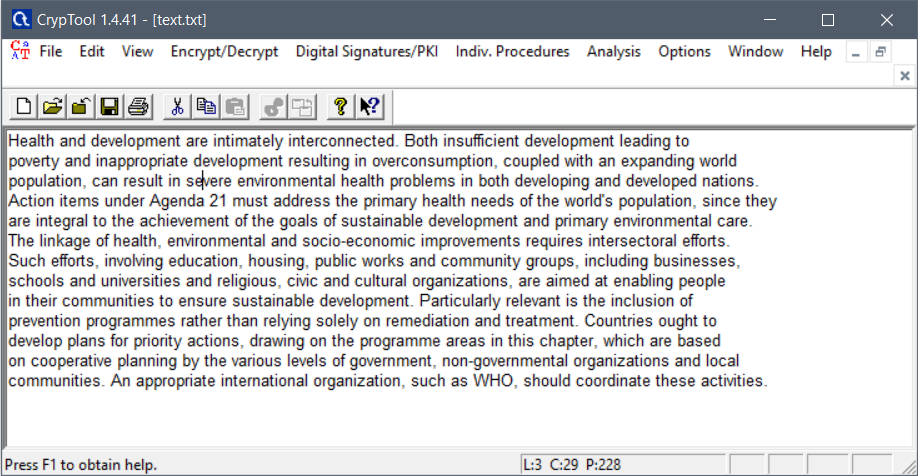


Рисунок 6 – Исходный текст

2. Создать бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.

Результат выполнения шифрования и расшифрования исходного текста шифром DES на 0-м ключе представлен на рис. 7.

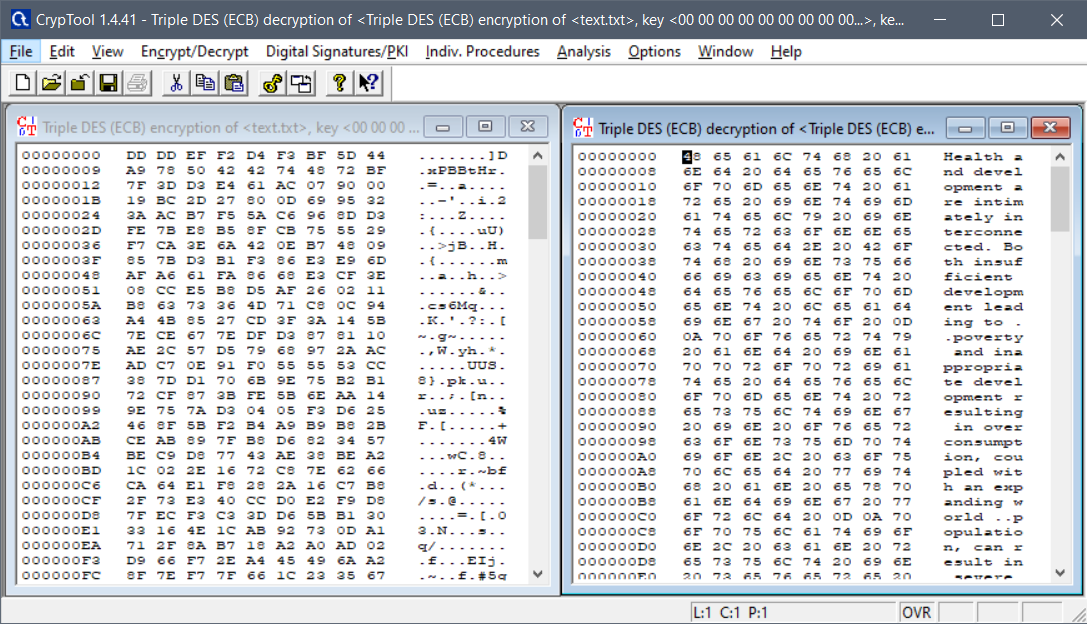


Рисунок 7 – Результат шифровки и расшифровки исходного текста на 0-м ключе

3. Снять и сохранить частотную и автокорреляционную характеристику этого файла.

Требуемые характеристики представлены на рис. 8 и 9.

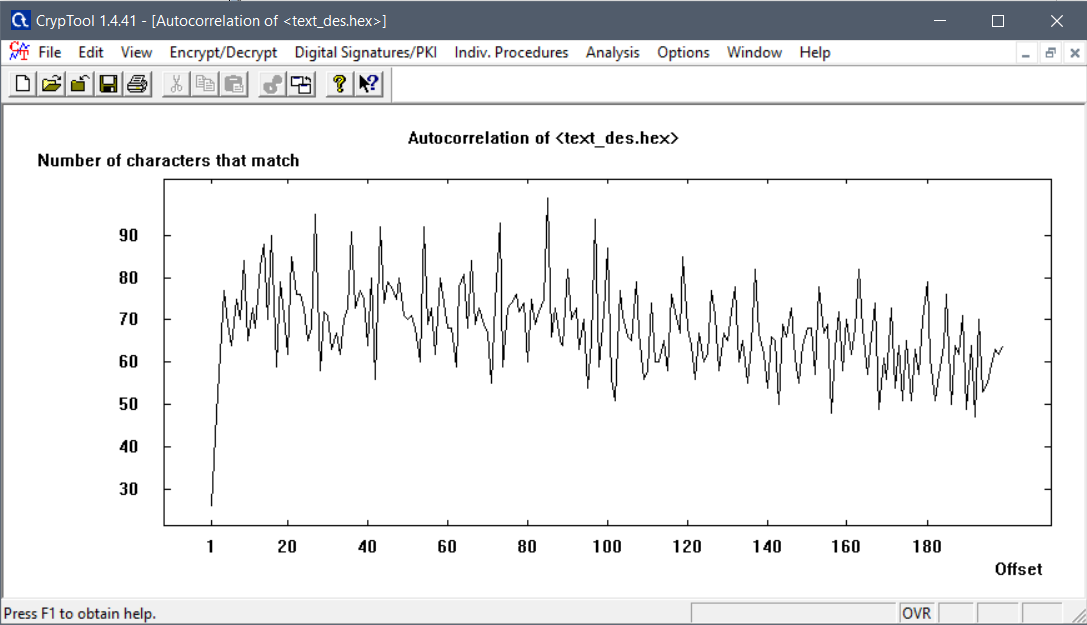


Рисунок 8 – Автокорреляционная характеристика

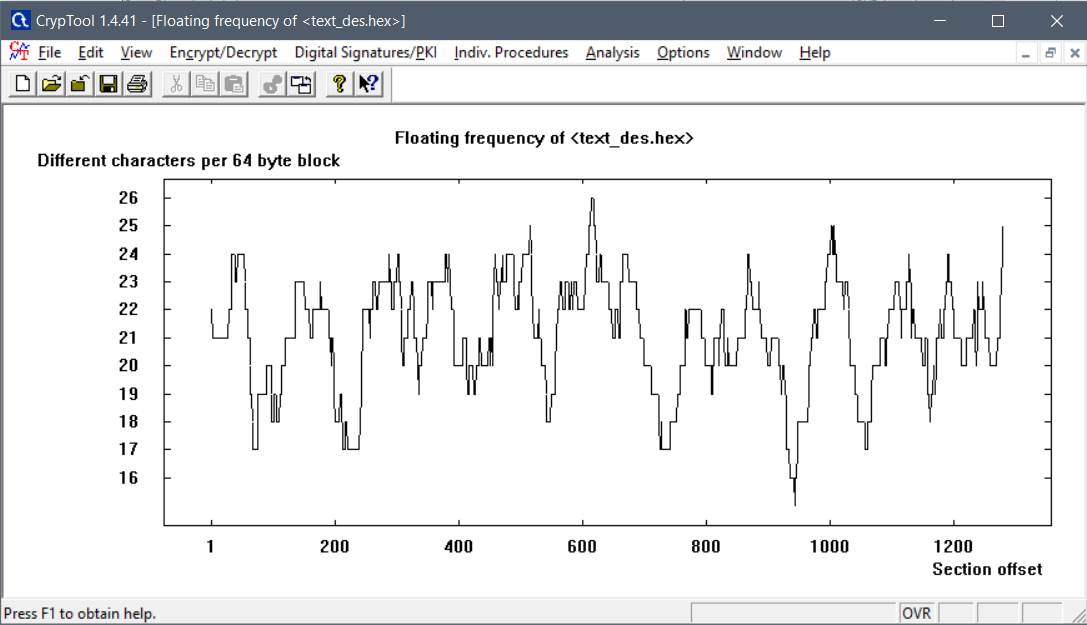
**

Рисунок 9 – Частотная характеристика

4. Зашифровать бинарный файл шифром 3-DES в режиме ECB.

Результат зашифровки представлен на рис. 10.

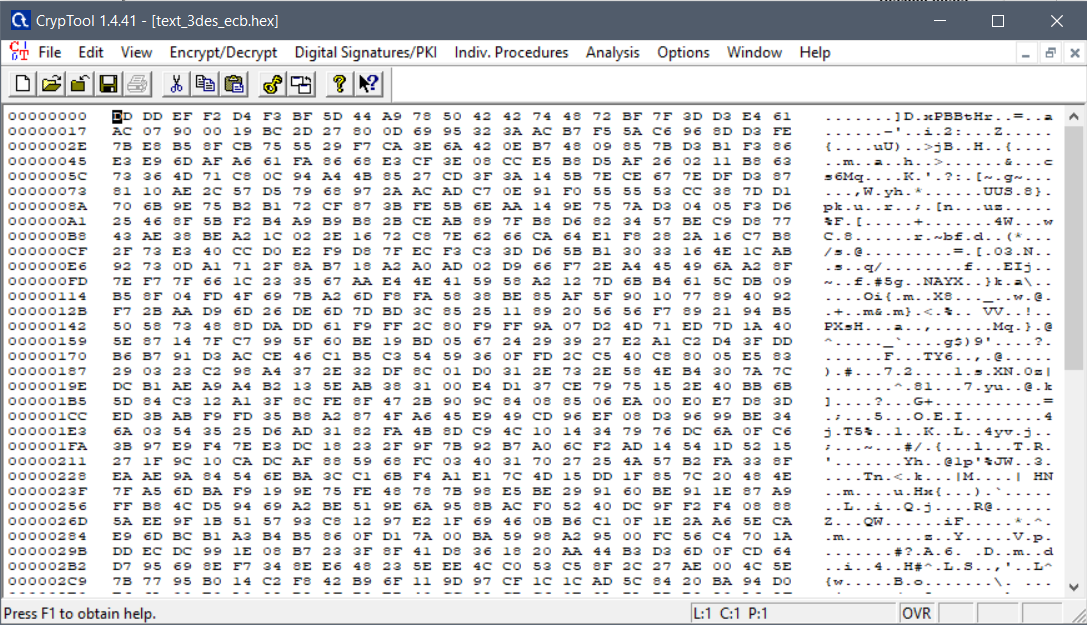


Рисунок 10 – Результат зашифровки исходного текста шифром 3-DES в режиме ECB

5. Снять и сохранить частотную и автокорреляционную характеристику файла с шифровкой.

Требуемые характеристики представлены на рис. 11 и 12 соответственно.

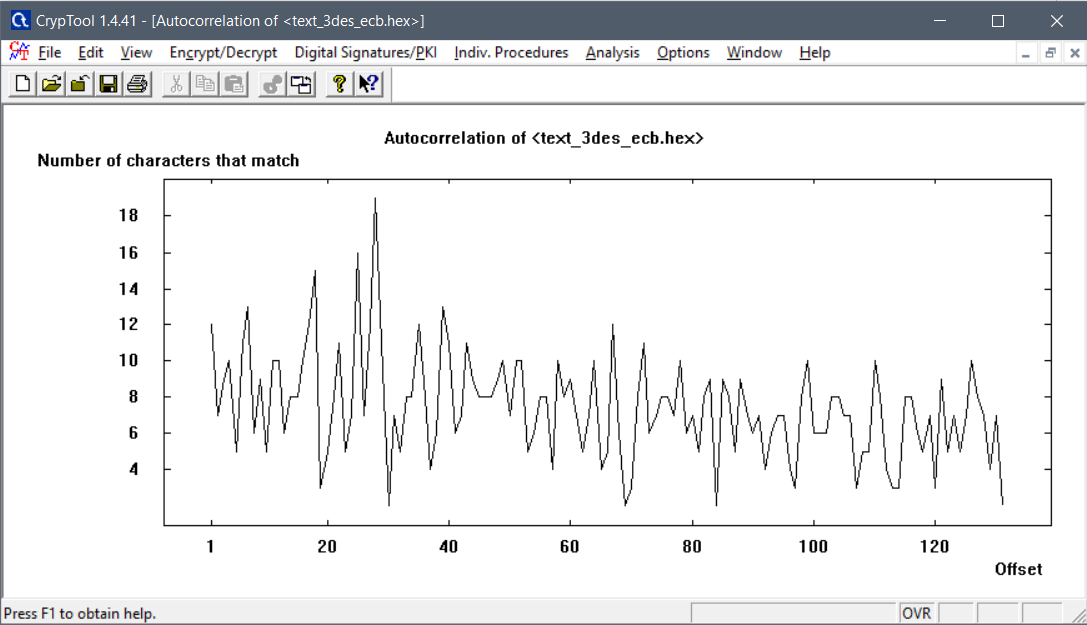


Рисунок 11 – Автокорреляционная характеристика

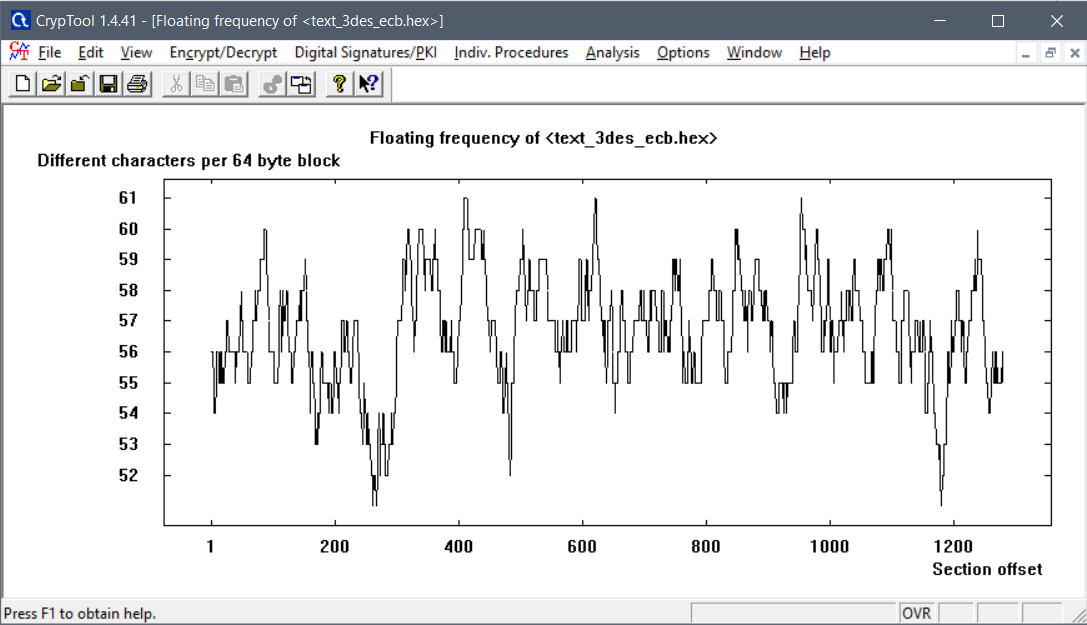
**

Рисунок 12 – Частотная характеристика

6. Зашифровать исходный бинарный файл 3-DES в режиме CBC c тем же ключом.

Результат зашифровки представлен на рис. 13.

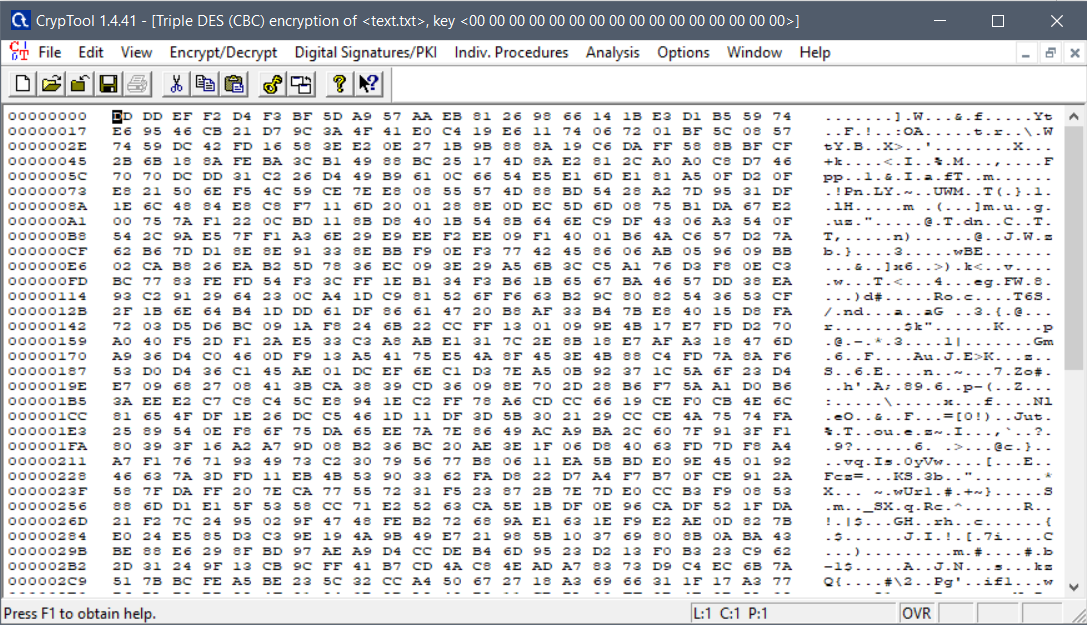


Рисунок 13 – Результат зашифровки исходного текста шифром 3-DES в режиме CBC

7. Снять и сохранить частотную и автокорреляционную характеристику файла с шифровкой.

Требуемые характеристики представлены на рис. 14 и 15 соответственно.

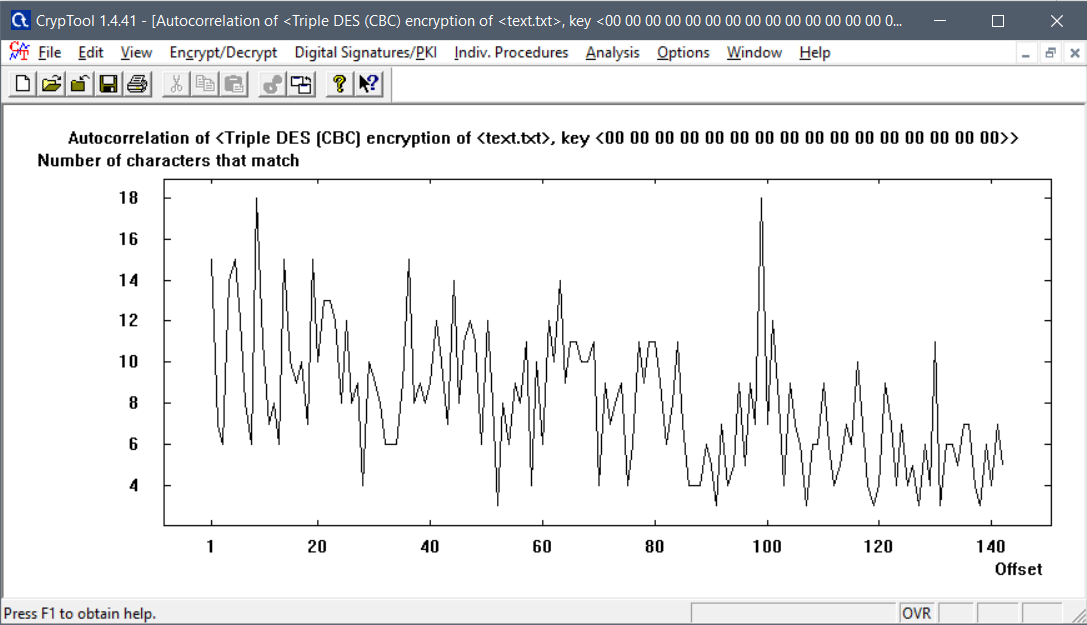


Рисунок 14 – Автокорреляционная характеристика

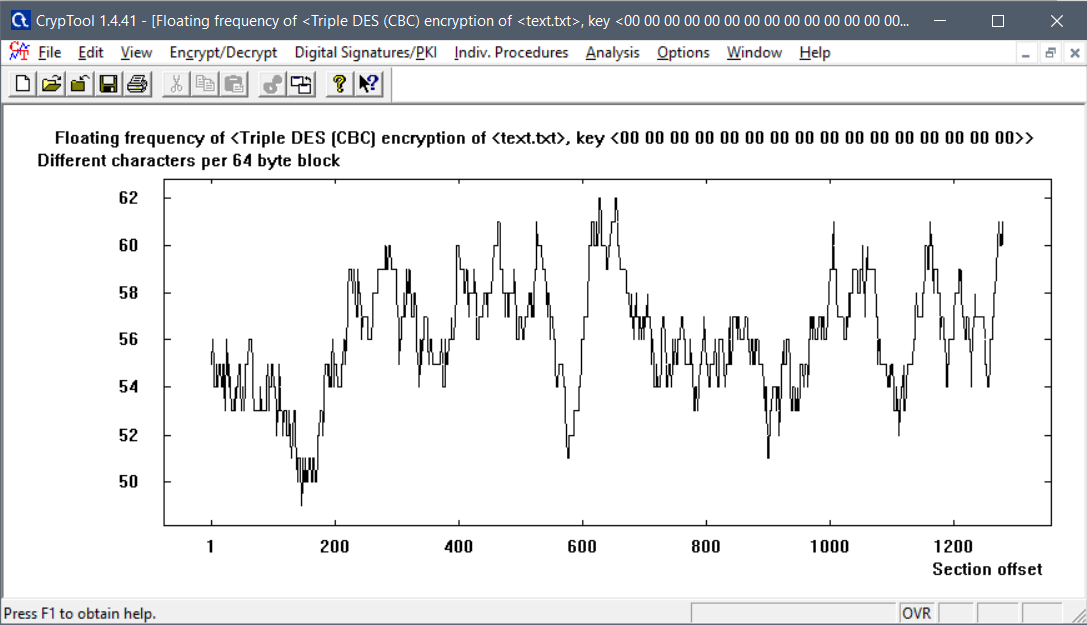
**

Рисунок 15 – Частотная характеристика

8. Определить экспериментальным путем по какой схеме работает реализация 3-DES в CrypTool. Сохранить подтверждающие скриншоты.

Чтобы определить по какой схеме работает реализация 3-DES в CrypTool рассмотрим по порядку шаги зашифровки.

В первую очередь внимание на длину ключа. В программе она равна 128 битам, но что более полезно для анализа – 112 бит настоящего ключа (без исключения битов четности).

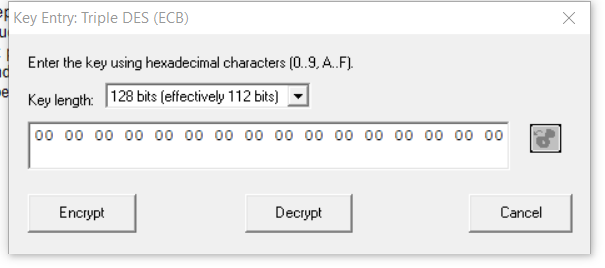


Рисунок 16 – Длина ключа в шифре 3-DES

Однако, если бы в приложении использовался бы DES-EEE3 или DES-EDE3, то длина ключа составила бы 168 бит (уже с исключением битов четности). Следовательно, реализован либо DES-EEE2, либо DES-EDE2 ().

Теперь необходимо определить уже из двух потенциальных вариантов. Пусть ключ на втором этапе в шифре DES-EDE2 совпадёт с ключом на первом этапе. Получится, что мы зашифруем текст, затем его расшифруем и снова зашифруем. В таком случае на выходе мы просто получим результат работы обычного DES. Такой ход можно проверить в программе.

Возьмем тот же ключ, что и в прошлых пунктах. Ключ – все нули.

Результат зашифровки представлен на рис. 17.

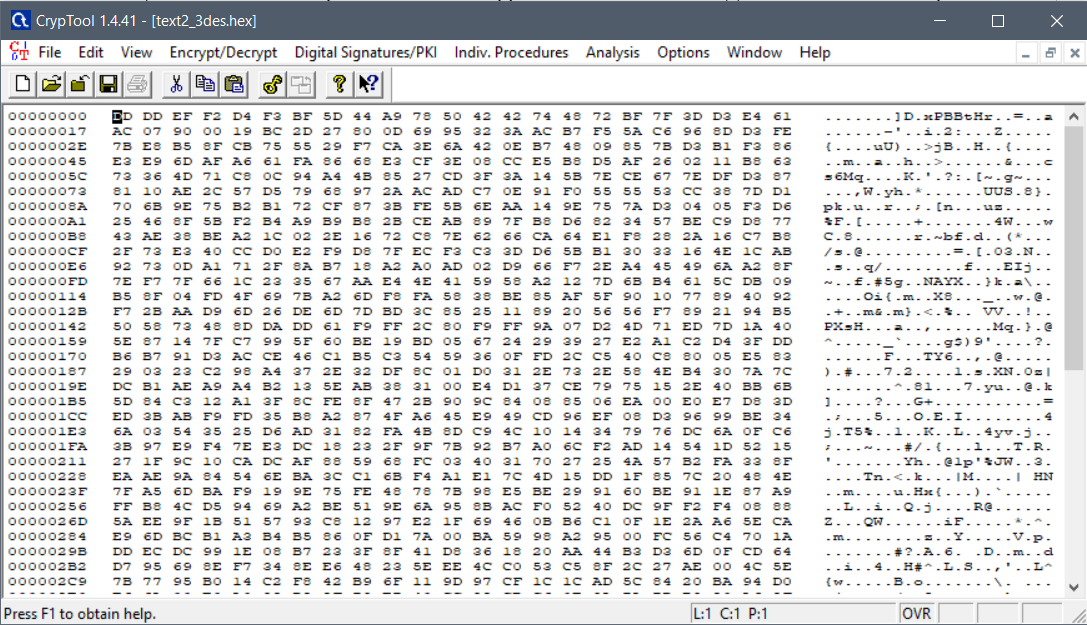
****

Рисунок 17 – Результат зашифровки

Рассмотрим теперь результат зашифровки обычным DES. Используем тот же ключ. После выполнения зашифровки шифротекст совпал, что продемонстрировано на рис. 18 (слева – DES, справа – 3DES). Значит в программе CrypTool используется DES-EDE2.

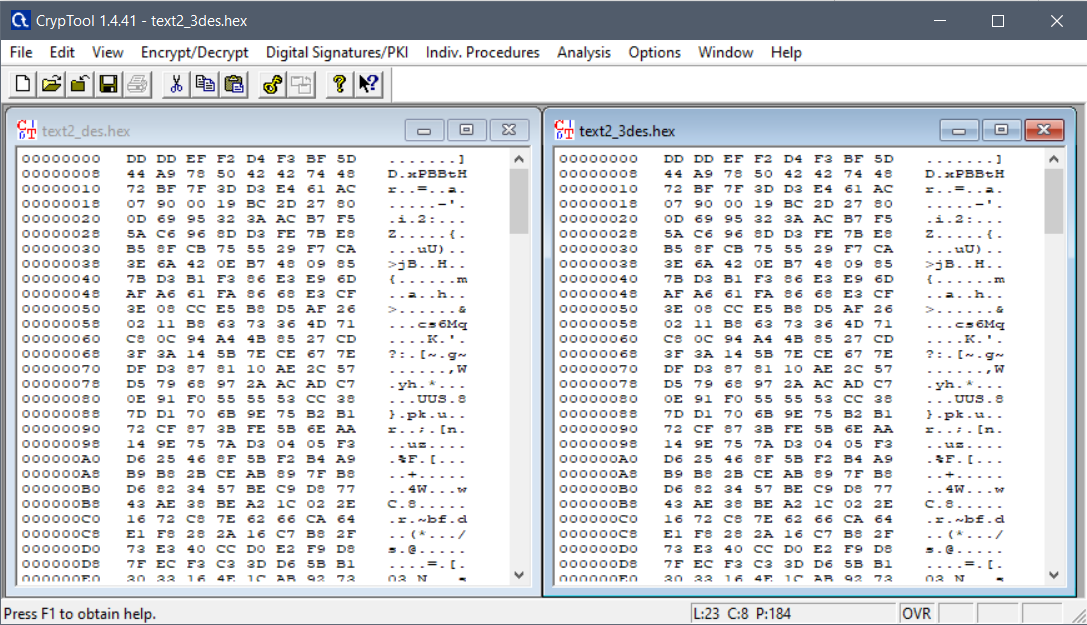
****

Рисунок 18 – Сравнение получившихся шифротекстов

Была проведена атака «грубой силы» в случаях, когда известна некоторая часть ключа. Результаты занесены в таблицу 4 и таблицу 5 соответственно (режимы ECB и CBC).

Таблица 4 – Зависимость времени расшифровки при известной части ключа (ECB)

|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 2 | года |
| 3 | года |
| 4 | года |
| 5 | года |
| 6 | года |
| 7 | года |
| 8 | года |
| 9 | года |
| 10 | года |
| 11 | дней |
| 12 | часа |
| 13 | секунд |
| 14 | секунд |
| 15 | < 1 секунды |

Таблица 5 – Зависимость времени расшифровки при известной части ключа (CBC)

|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 2 | года |
| 3 | года |
| 4 | года |
| 5 | года |
| 6 | года |
| 7 | года |
| 8 | года |
| 9 | года |
| 10 | года |
| 11 | дней |
| 12 | часа |
| 13 | секунд |
| 14 | секунда |
| 15 | < 1 секунды |

***Исследование модификаций DESX, DESL, DESXL шифра DES.***

*Основные параметры и обобщенные схемы шифров.*

Алгоритм DESX использует на входе ключ длиной 184 бита, который делится на 3 56-битные части. Процесс шифрования происходит по следующей схеме:

Если , то данный алгоритм сводится к стандартному DES.

Алгоритм DESL является облегченной версией алгоритма DES. Данный алгоритм был создан в 2006 году для RFID-меток. Алгоритм предполагает отказ от входной и выходной перестановки блока текста, т.к. они не несут криптографической сложности, а также 8 S-блоков заменяется на 1, но более стойкий чем все 8 стандартных блока DES.

Алгоритм DESXL использует те же оптимизации что и DESL, но производит шифрование по алгоритму DESX.

1. Выбрать случайный текст на английском языке (не менее 1000 знаков).

Был выбран тот же текст, что и в пункте 2.6.

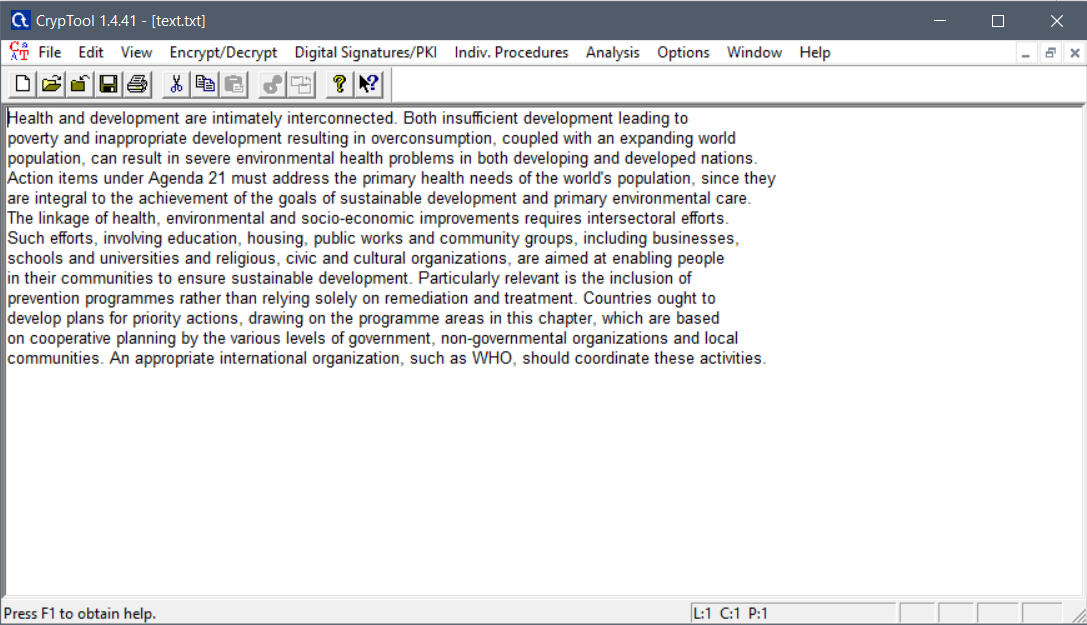


Рисунок 19 – Исходный текст

1. Создать бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.

Результат выполнения шифрования и расшифрования исходного текста шифром DES на 0-м ключе представлен на рис. 20.

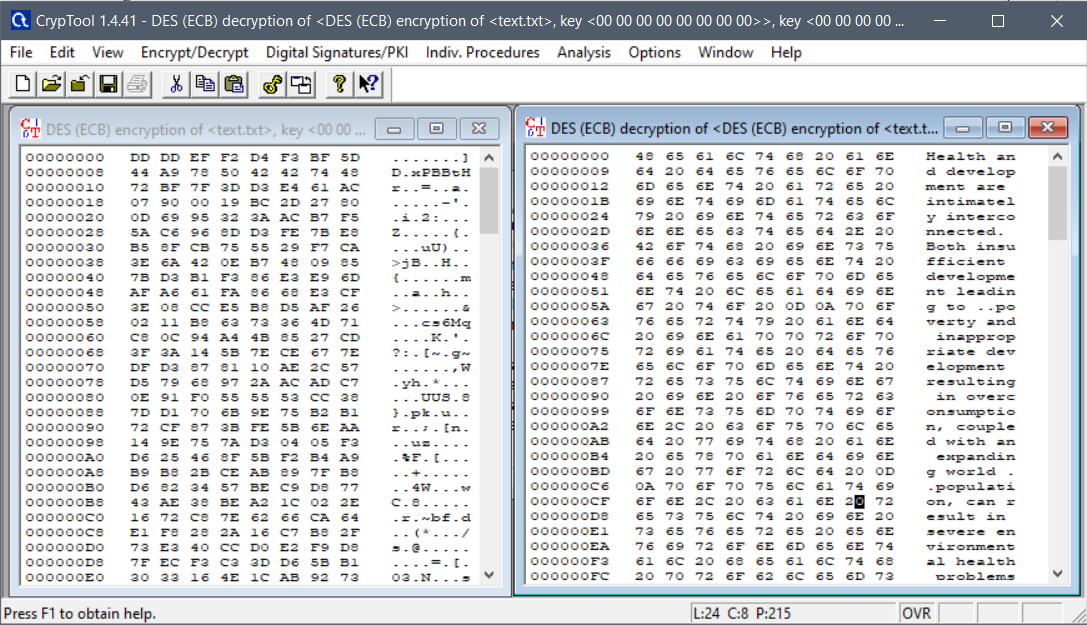


Рисунок 20 – Результат шифровки и расшифровки исходного текста на 0-м ключе

1. С помощью CrypTool зашифровать текст с использованием шифров DESX, DESL, DESXL.

Выбранный ключ: ABDBADBFAF13413B235B2C452C5BCB245BC245BC25B2C45B

Зашифруем исходный текст с использованием шифра DESX. Результат шифрования представлен на рис. 21.

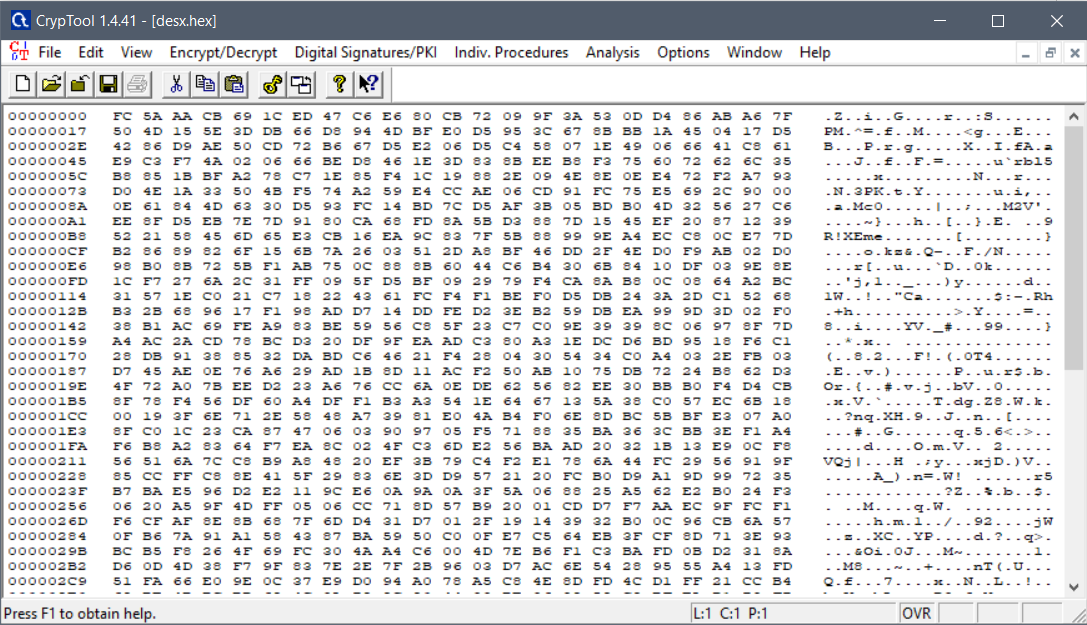


Рисунок 21 – Результат зашифровки исходного текста шифром DESX

Зашифруем исходный текст с использованием шифра DESL. Результат шифрования представлен на рис. 22.



Рисунок 22 – Результат зашифровки исходного текста шифром DESL

Зашифруем исходный текст с использованием шифра DESXL. Результат шифрования представлен на рис. 23.

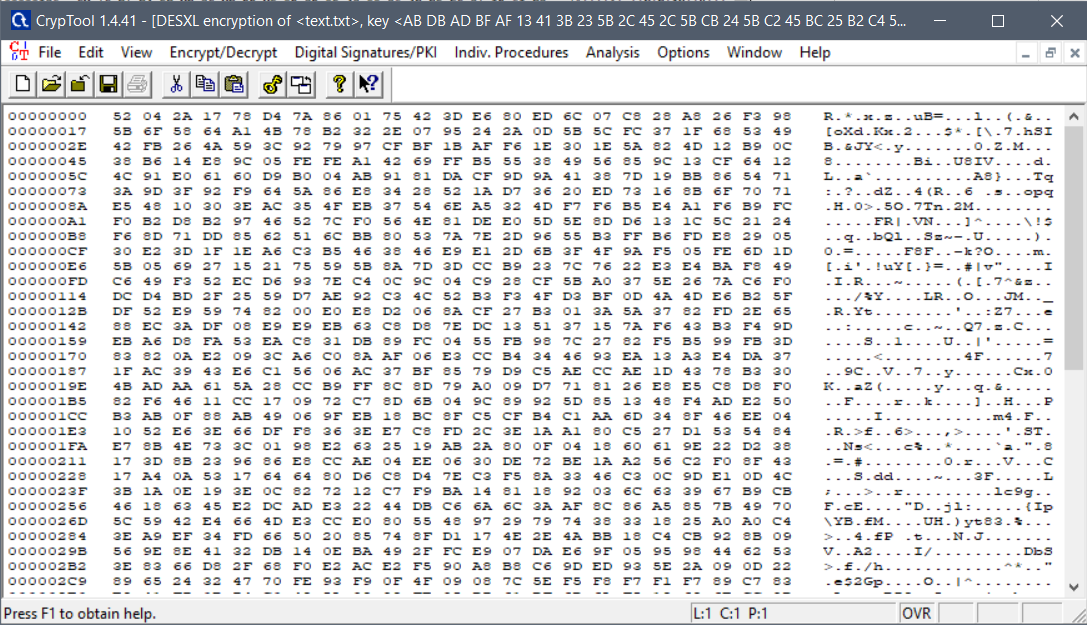


Рисунок 23 – Результат зашифровки исходного текста шифром DESXL

1. Средствами CrypTool вычислить энтропию исходного текста и шифротекстов, полученных в итоге. Зафиксировать результаты измерений в таблице.

Вычислим энтропию исходного текста. Результат представлен на рис. 24.

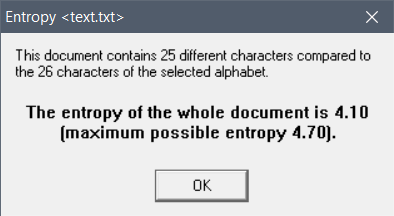


Рисунок 24 – Значение энтропии для исходного текста

Вычислим энтропию шифротекста, зашифрованного DESX. Результат представлен на рис. 25.

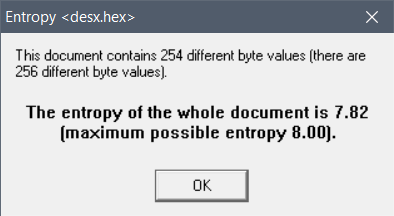


Рисунок 25 – Значение энтропии для текста, зашифрованного шифром DESX

Вычислим энтропию шифротекста, зашифрованного DESL. Результат представлен на рис. 26.

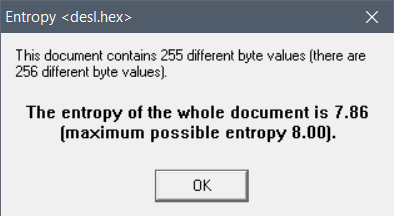


Рисунок 26 – Значение энтропии для текста, зашифрованного шифром DESL

Вычислим энтропию шифротекста, зашифрованного DESXL. Результат представлен на рис. 27.

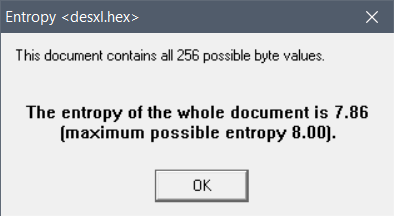


Рисунок 27 – Значение энтропии для текста, зашифрованного шифром DESXL

Сведем полученные значения в таблицу 6.

Таблица 6 – Значение энтропии для исходного текста и трёх шифров (DESX, DESL, DESXL)

|  |  |
| --- | --- |
| *Название шифра* | *Значение энтропии* |
| *Исходный текст* | 4.10 |
| *DESX* | 7.82 |
| *DESL* | 7.86 |
| *DESXL* | 7.86 |

1. Средствами CrypTool оцените время проведения атаки «грубой силы» при полном отсутствии информации о секретном ключе.

Проведем атаку грубой силы при полном отсутствии информации о секретном ключе и сведем полученные значения в таблицу 7.

Таблица 7 – Зависимости времени подбора ключа от используемого шифра

|  |  |
| --- | --- |
| *Название шифра* | *Время расшифровки* |
| *DESX* | лет |
| *DESL* | лет |
| *DESXL* | лет |

**Выводы.**

* Изучен демонстрационный пример шифра DES, представленный в CrypTool. Выполнен ручной расчет субблоков и раундовых ключей шифра для первых двух раундов. Ключ и исходный текст были заданы.
* Изучены два режима шифра DES – ECB и CBC.
  1. При использовании шифра DES в режиме ECB блоки кодируются независимо с использованием одного и того же ключа шифрования, благодаря чему сохраняется однородность зашифрованных данных там, где она присутствовала в исходном изображении. Однородные данные хорошо подаются сжатию с одной стороны, и проще в расшифровке с другой.
  2. При использовании режима CBC изображение превращается в шум. Однако такие неоднородные данные почти не поддаются сжатию.
* Проведены попытки взлома ключа методом “грубой силы” в режимах ECB и CBC.
  1. Были выявлены закономерности:
     1. Если известная длина ключа составляет до 4 байт включительно, то скорость атаки на шифротекст в режиме CBC возрастает в полтора-два раза.
     2. С уменьшением известной длины ключа скорость атаки в обоих случаях существенно понижается.
* Рассмотрен шифр 3-DES в четырех его версиях.
  1. Экспериментальным путем была выявлена используемая в программе CrypTool реализация 3-DES – DES-EDE2.
* Проведены попытки взлома ключа методом “грубой силы” шифра 3-DES.
  1. В ходе анализа атаки “грубой силой” шифра 3-DES в режимах ECB и CBC было выявлено, что шифр является довольно безопасным, так как, зная 10 байт из возможных 16, время дешифровки займет больше двух лет.
* Изучены шифры DESX, DESL, DESXL.
  1. Выявлено, что шифрование DESX, DESL, DESXL имеет примерно одинаковую эффективность. Эти значения примерно в два раза больше, чем у исходного текста, что означает внешнюю псевдослучайность шифротекста.
* Исследовано время расшифровки текста при полном отсутствии информации о секретном ключе.
  1. Шифры DESX и DESXL показали гораздо лучший результат, чем шифр DESL.