МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра информационной безопасности

ОТЧЕТ

по лабораторной работе №5
по дисциплине «Криптография и защита информации»
Тема: Изучение шифра AES

Студент гр. 8383 _____ Киреев К.А.

Преподаватель _____ Племянников А.К.

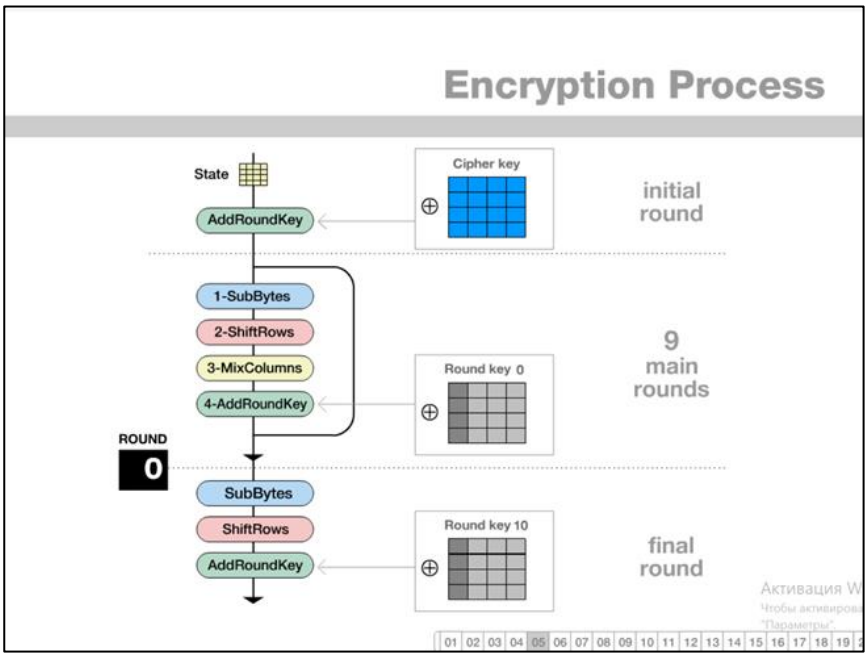
Санкт-Петербург
2021

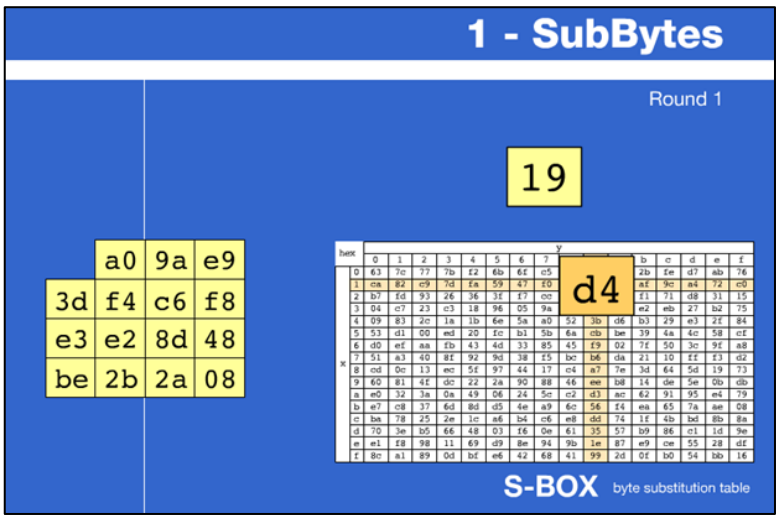
Цель работы.

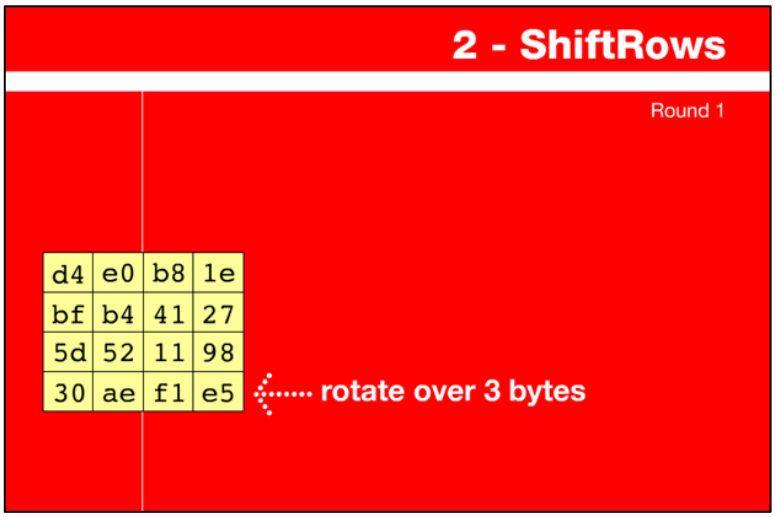
Исследовать характеристики шифра AES и финалистов конкурса AES, а также изучить атаку предсказанием дополнения и получить практические навыки работы с шифрами и проведения атаки, в том числе с использованием приложения Cryptool 1 и 2.

Исследование преобразований AES.

1. Изучить преобразования шифра AES с помощью демонстрационного приложения из `Cryptool 1: Indiv.Procedures->Visualization…->AES->Rijndael Animation.`







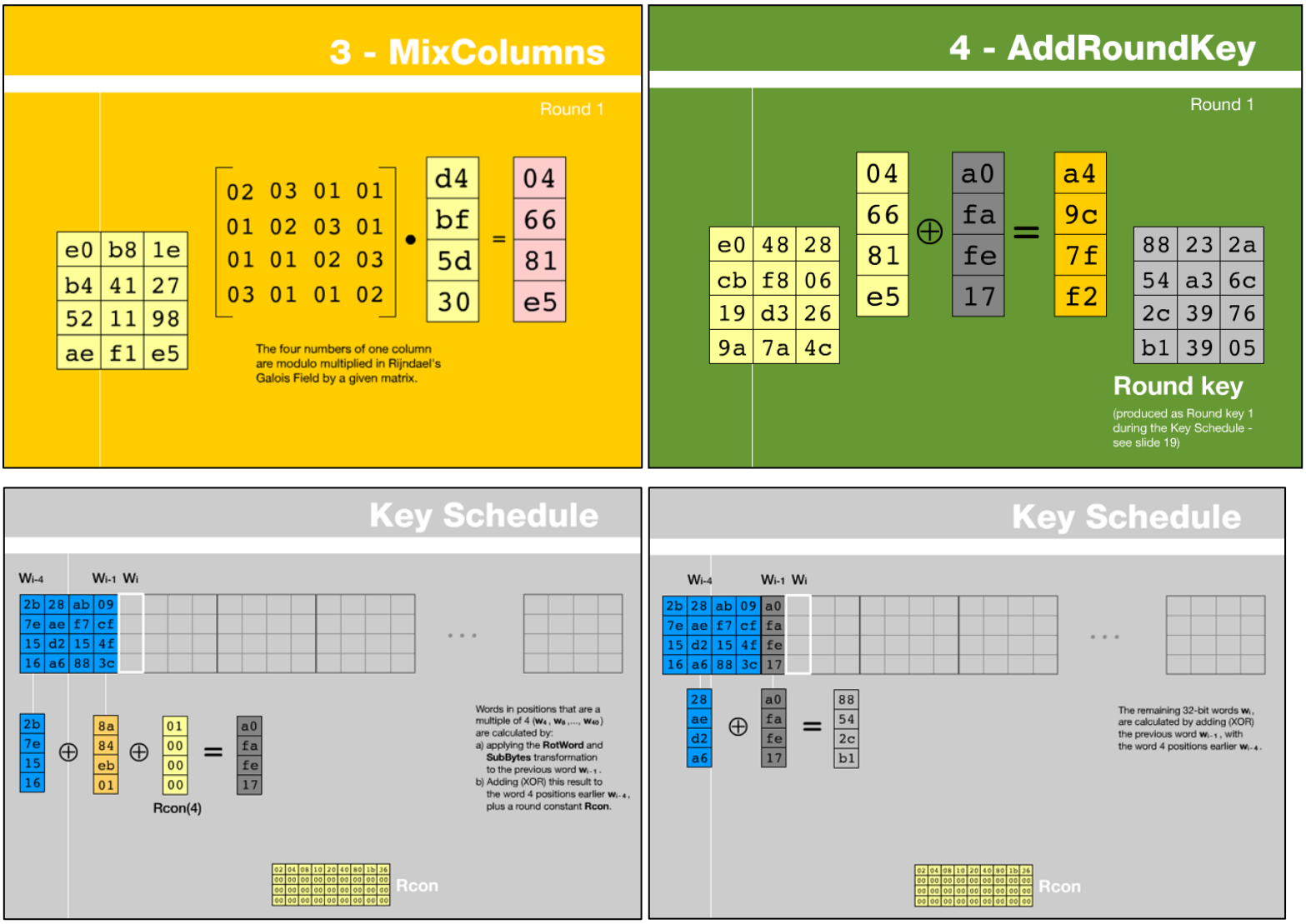


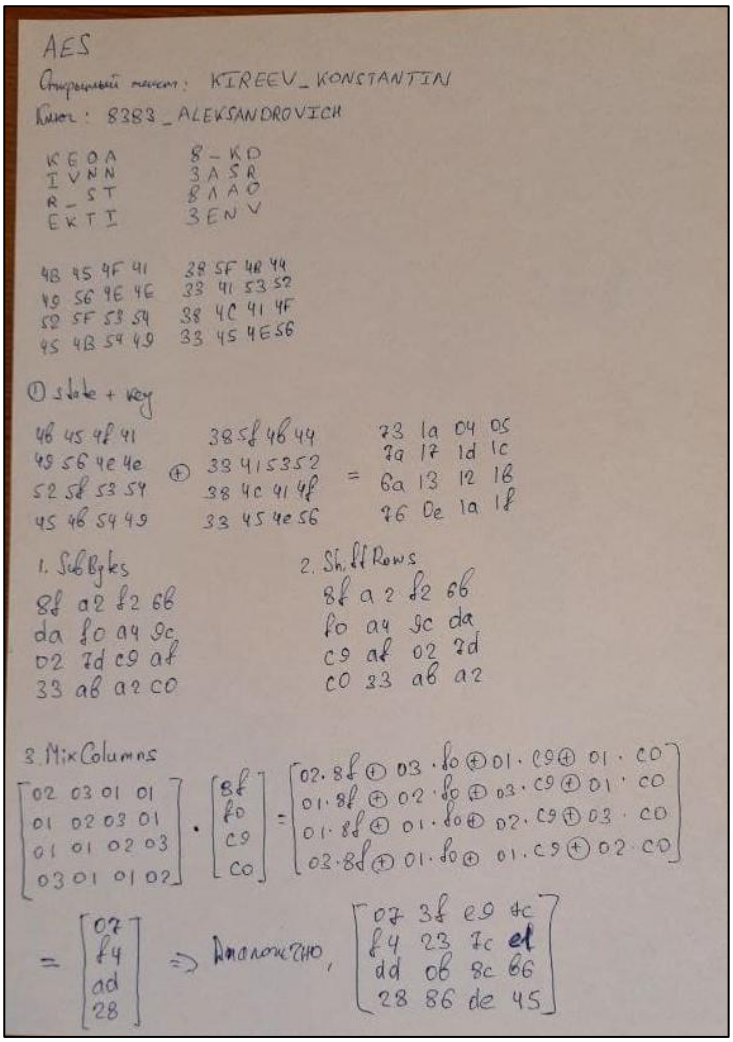
Рисунок 1 – Запуск демонстрационного примера

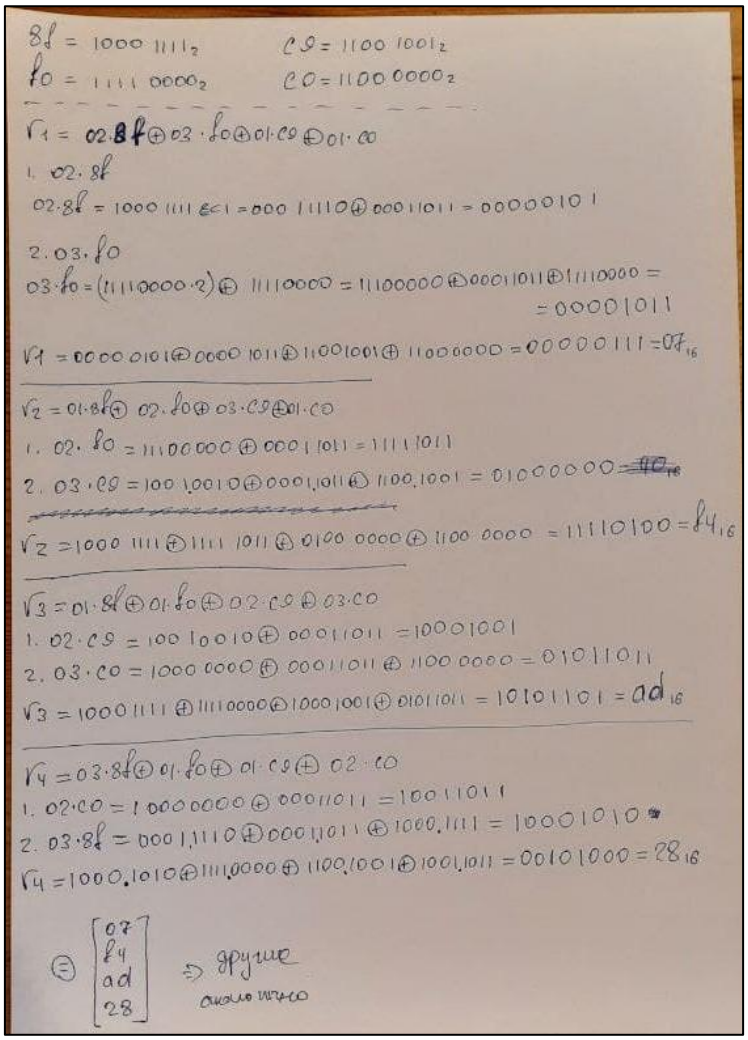
2. Выполнить вручную преобразования для одного раунда и вычисление раундового ключа при следующих исходных данных:

a. Открытый текст – фамилия_имя (транслитерация латиницей)

b. Ключ – номер группы_отчество

Было выполнено ручное преобразование для одного раунда и вычисление раундового ключа при заданных исходных данных. Результат представлен на рис. 2.





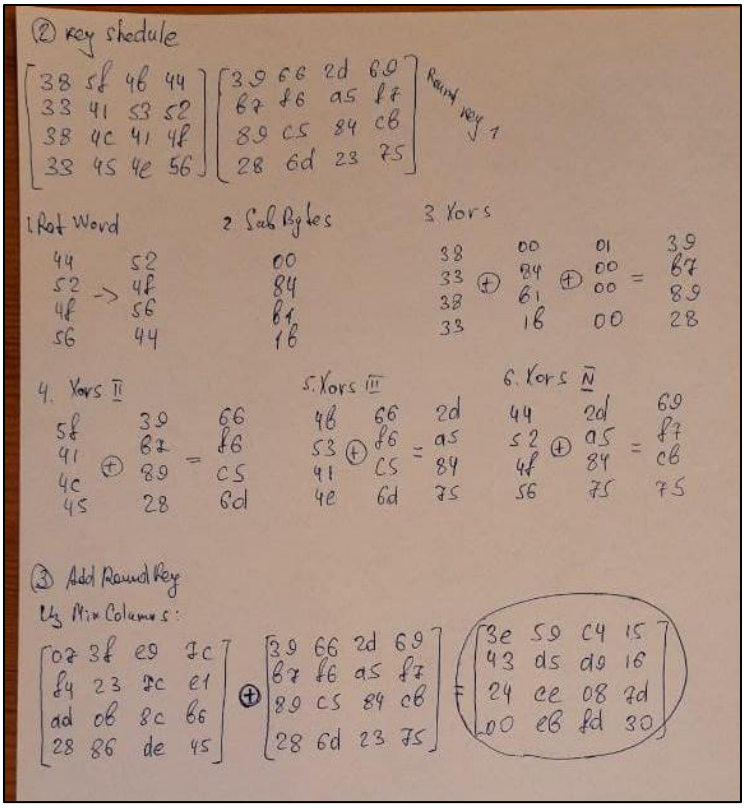


Рисунок 2 – Ручное преобразование шифра AES

3. Проверить полученные результаты с помощью приложения-инспектора: Indiv.Procedures->Visualization…->AES->Rijndael Inspector.

Была выполнена проверка ручных расчетов через CrypTool. Из рис. 3 видно, что результаты совпали.

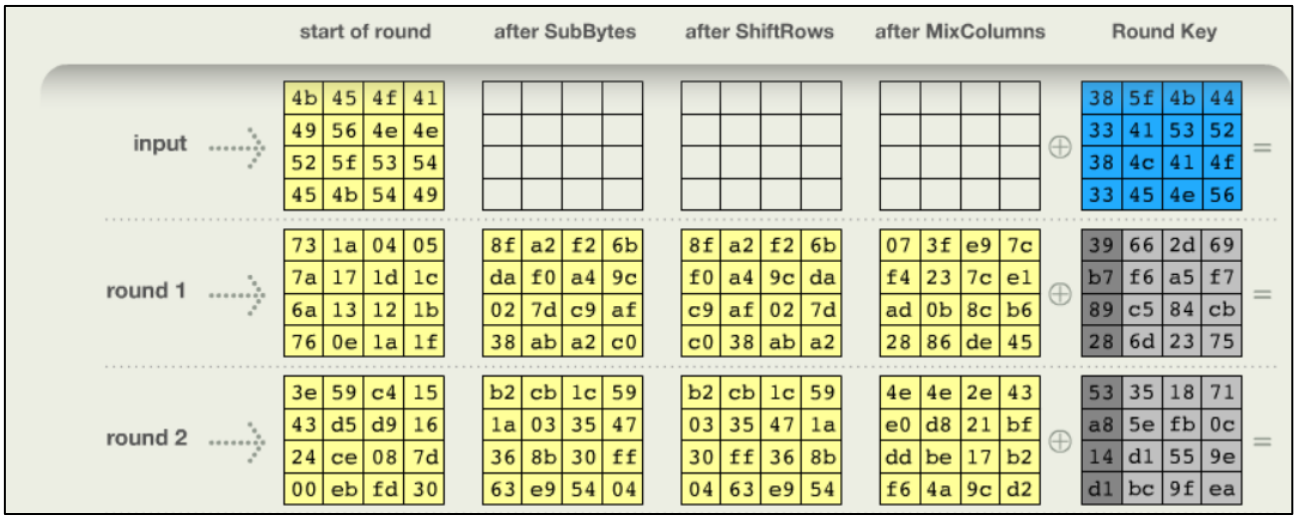


Рисунок 3 – Раундовое шифрование AES в CrypTool

4. Провести наблюдения в потоковой модели шифра AES с помощью демонстрационного приложения из CrypTool 1 для 0-текста и 0-ключа: Indiv.Procedures->Visualization…->AES->Rijndael Flow Visualisation.

Был запущен шифр AES для 0-текста и 0-ключа через Rijndael Flow Visualisation. Результат представлен на рис.4.

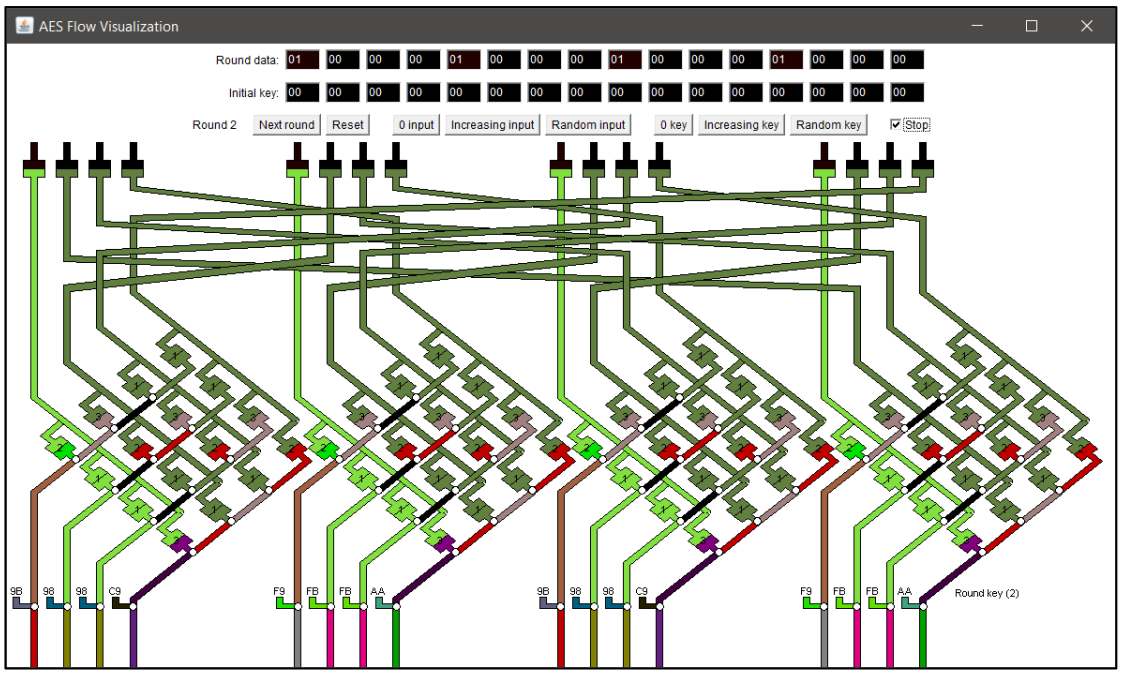


Рисунок 4 – Rijndael Flow Visualisation для 0-текста и 0-ключа

Исследование финалистов конкурса AES (Rijndael, MARS, RC6, Serpent, Twofish).

1. Выбрать текст на английском языке (не более 120 знаков).

Для изучения других шифров финалистов конкурса был выбран фрагмент из файла English.txt, представленный на рис. 5.

Рисунок 5 – Исходный текст

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

Было выполнено шифрование исходного текста с 0-ключом. Результат представлен на рис.6.

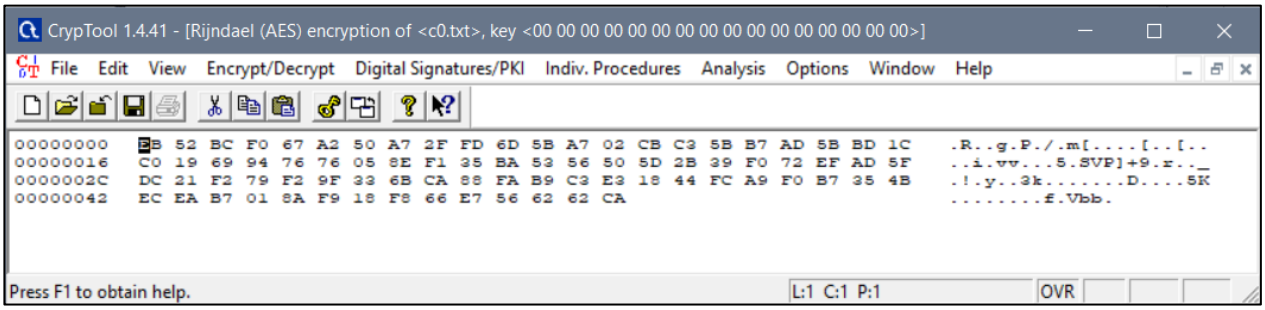


Рисунок 6 – Шифрование с 0-ключом

3. С помощью Cryptool 1 зашифровать с ключом отличным от 0 текст с использованием шифров AES, MARS, RC6, Serpent и Twofish.

Было выполнено шифрование исходного текста с выбранным ключом (383338335F414C454B53414E44524F56) шифрами AES, MARS, RC6, Serpent и Twofish.

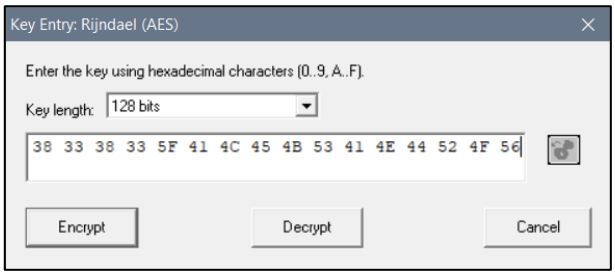


Рисунок 7 – Исходный ключ

Результаты представлены на рис. 8 – 12 соответственно.

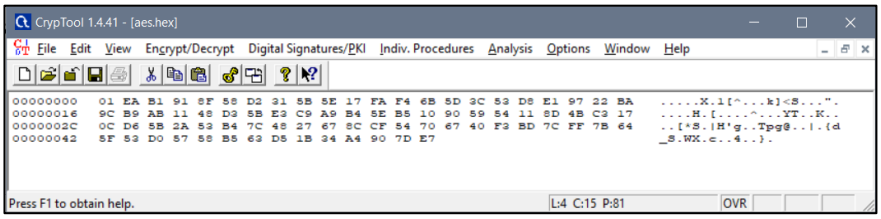


Рисунок 8 – Результат работы шифра AES

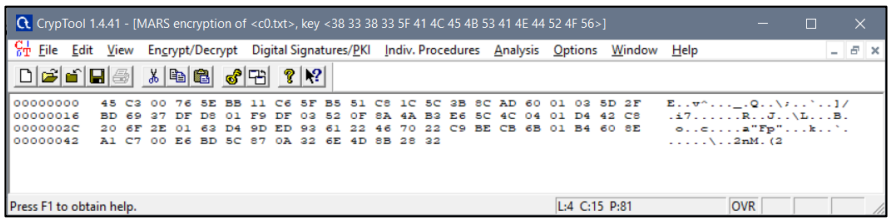


Рисунок 9 – Результат работы шифра MARS

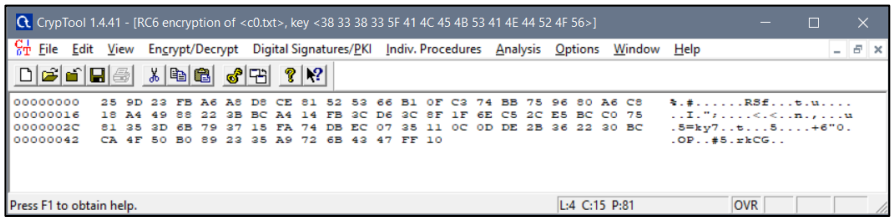


Рисунок 10 – Результат работы шифра RC6

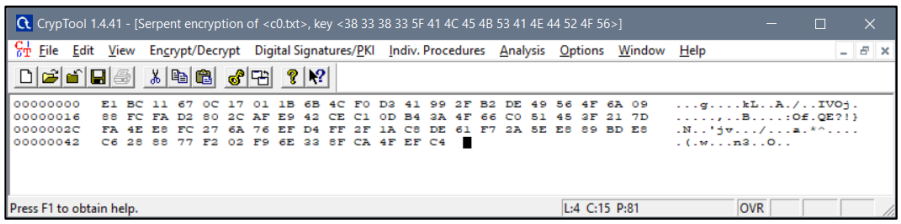


Рисунок 11 – Результат работы шифра Serpent

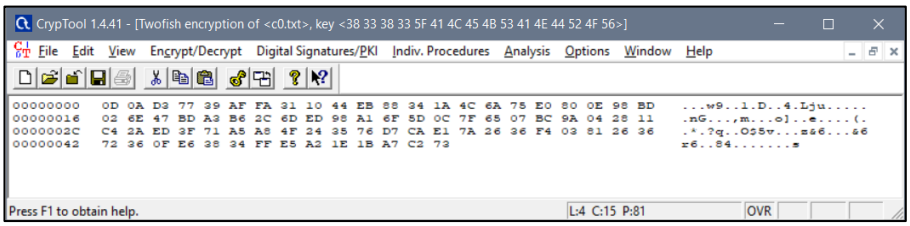


Рисунок 12 – Результат работы шифра Twofish

4. Приложением из Cryptool 1 вычислить энтропию исходного текста и шифротекстов, полученных в итоге. Зафиксировать результаты измерений в таблице.

Результаты вычислений энтропии для каждого из исследуемых шифров представлены в таблице 1.

Таблица 1 – Значение энтропии для каждого из шифров

Название шифра	***Энтропия***
Исходный текст	3.72
AES	5.92
MARS	5.86
RC6	5.95
Serpent	6.02
Twofish	6.13

5. Приложением из Cryptool 1 оцените время проведения атаки «грубой силы» всех шифров для одного и того же шифротекста в случаях, когда известно n-2, n-4, n-6, ..., 2 байт секретного ключа. Зафиксировать результаты измерений в таблице.

Была выполнена атака «грубой силы» когда известна некоторая часть секретного ключа. Результаты приведены в таблице 2.

Таблица 2 – Зависимость времени расшифровки при известной части ключа

Количество известных байт	***AES***	***MARS***	***RC6***	***Serpent***	***Twofish***
14	менее секунды	менее секунды	менее секунды	менее секунды	менее секунды
12	1.04 часа	1.07 час	1.05 часа	1.04 часа	1.02 часа
10	7.9 лет	9 лет	7.9 лет	7.9 лет	14 лет
8	5.3e + 005 лет	5.5e + 006 лет	5.5e + 005 лет	5.2e + 006 лет	5.5e + 006 лет

6	3.5e + 010 лет	3.6e + 010 лет	3.7e + 010 лет	3.4e + 011 лет	3.3e + 010 лет
4	2.4e + 015 лет	2.5e + 015 лет	2.2e + 015 лет	2.2e + 015 лет	2.3e + 015 лет
2	1.6e + 020 лет	1.5e + 020 лет	1.7e + 020 лет	1.5e + 020 лет	1.5e + 020 лет

Атака «грубой силы» на AES.

1. Найти и запустить шаблон атаки в CrypTool 2: AES Analysis using Entropy(2).

Был изучен шаблон атаки на шифр AES с использованием энтропии. Шаблон представлен на рис. 12.

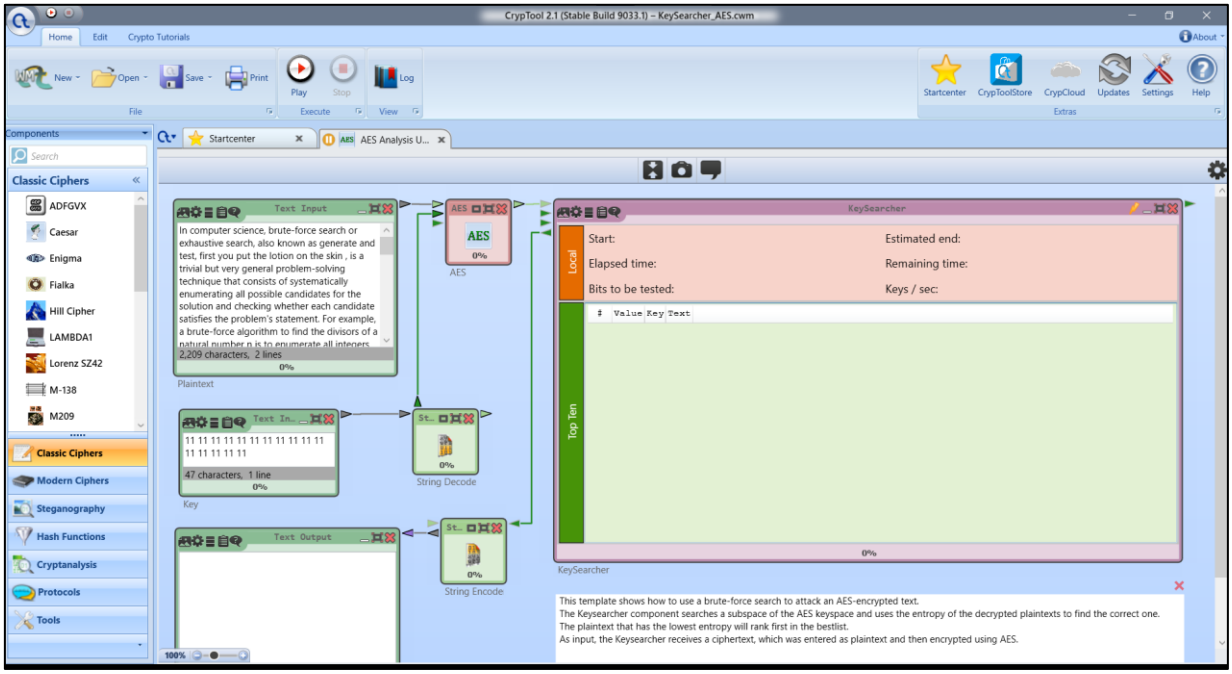


Рисунок 12 – Шаблон атаки AES Analysis using Entropy

2. Выбрать открытый текст (примерно 1000 знаков) и загрузить его в шаблон.

Исходный текст представлен на рис. 13. Ключ - 383338335F414C454B53414E44524F56.

Economic policies of individual countries and international economic relations both have great relevance to sustainable development. The reactivation and acceleration of development requires both a dynamic and a supportive international economic environment and determined policies at the national level. It will be frustrated in the absence of either of these requirements. A supportive external economic environment is crucial. The development process will not gather momentum if the global economy lacks dynamism and stability and is beset with uncertainties. Neither will it gather momentum if the developing countries are weighted down by external indebtedness, if development finance is inadequate, if barriers restrict access to markets and if commodity prices and the terms of trade of developing countries remain depressed. The record of the 1980s was essentially negative on each of these counts and needs to be reversed.

Рисунок 13 – Исходный текст

3. Провести атаку «грубой силы» когда известно n-2, n-4, n-6 байт секретного ключа, используя в качестве оценочной функции энтропию и задействовав 1 ядро процессора. Зафиксировать затраты времени.

Установим требуемые параметры в программе и исследуем затраты времени. Результаты сведем в таблицу 3.

4. Выполнить атаку повторно с средним и максимальным количеством процессорных ядер. Зафиксировать затраты времени.

Установим требуемые параметры в программе и исследуем затраты времени. Результаты сведем в таблицу 3.

Таблица 3 – Зависимость затрат времени при различных известных частях ключа и количестве используемых ядер при атаке «грубой силой»

Известная часть ключа, байт	*Время атаки грубой силы*			
	Количество ядер			
	1	3	6	8
14	1 секунда	1 секунда	1 секунда	1 секунда
12	2 час 16 минут	52 минуты	38 минут	26 минут
10	7112 дней	2368 дней	1381 день	1157 дней

5. Сформировать текст с произвольным сообщением в формате «DEAR SIRS message THANKS» и загрузить его в шаблон.

Результат нового исходного текста представлен на рис. 14.

DEAR SIRS of individual countries and international economic relations both have great relevance to sustainable development. The reactivation and acceleration of development requires both a dynamic and a supportive international economic environment and determined policies at the national level. It will be frustrated in the absence of either of these requirements. A supportive external economic environment is crucial. The development process will not gather momentum if the global economy lacks dynamism and stability and is beset with uncertainties. Neither will it gather momentum if the developing countries are weighted down by external indebtedness, if development finance is inadequate, if barriers restrict access to markets and if commodity prices and the terms of trade of developing countries remain depressed. The record of the 1980s was essentially negative on each of these counts and needs to be THANKS

Рисунок 14 – Исходный текст

6. Провести атаку «грубой силы» когда известно n-2, n-4, n-6 байт секретного ключа, используя в качестве оценочной функции словосочетание DEAR SIRS задействовав 1 ядро процессора. Зафиксировать затраты времени.

Установим требуемые параметры в программе и исследуем затраты времени. Результаты сведем в таблицу 4.

7. Выполнить атаку повторно с средним и максимальным количеством процессорных ядер. Зафиксировать затраты времени.

Установим требуемые параметры в программе и исследуем затраты времени. Результаты сведем в таблицу 4.

Таблица 4 – Зависимость затрат времени при различных известных частях ключа с использованием оценочной функции и количестве используемых ядер при атаке «грубой силой»

Известная часть ключа, байт	*Время атаки грубой силы*			
	Количество ядер			
	1	3	6	8
14	1 секунда	1 секунда	1 секунда	1 секунда
12	1 час 4 минуты	25 минут	16 минут	14 минут
10	3827 дней	1184 дней	789 дней	700 дней

Атака предсказанием дополнения на шифр AES в режиме CBC (Padding Oracle Attack).

1. Найти и запустить шаблон атаки в CrypTool 2: *Padding Oracle Attack on AES.*

Был запущен шаблон атаки POA с заданными исходными данными. Результат работы шаблона представлен на рис. 15.

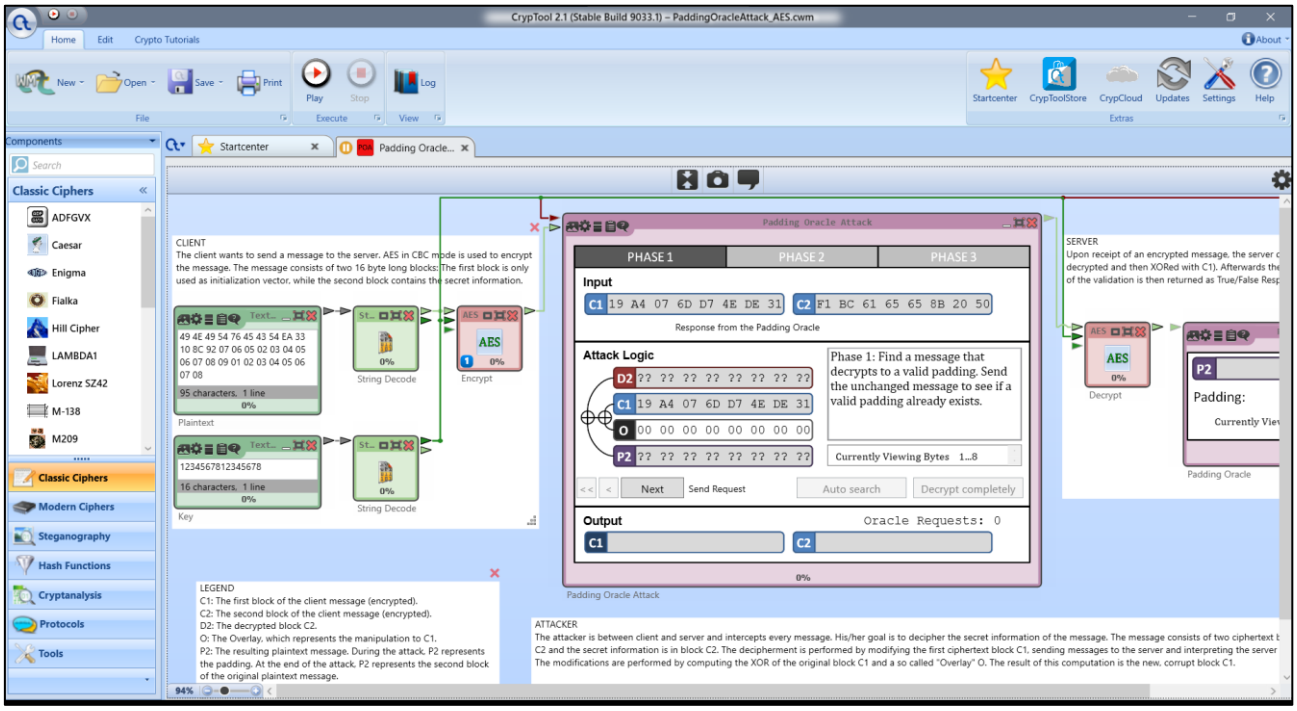


Рисунок 15 – Шаблон атаки POA

2. Подготовьтесь к атаке теоретически:

a. Изучите комментарии к шаблону

b. Изучите публикацию

3. Внедрите во второй блок исходного текста коды символов своего имени.

Результат изменения исходного текста представлен на рис. 16.

```
49 4E 49 54 76 45 43 54 EA 33 10 8C 92 07 06 05 02 03 04 05 06 07 08 09 4e 02 4f 04 4b 49 07 54
```

Рисунок 16 – Изменённый исходный текст

4. Выполните 3 фазы атаки и сохраните итоговые скриншоты по окончанию каждой фазы.

Используя секретный ключ – 1234567812345678 проведем 3 фазы атаки. Результаты каждой фазы представлены на рис. 17.

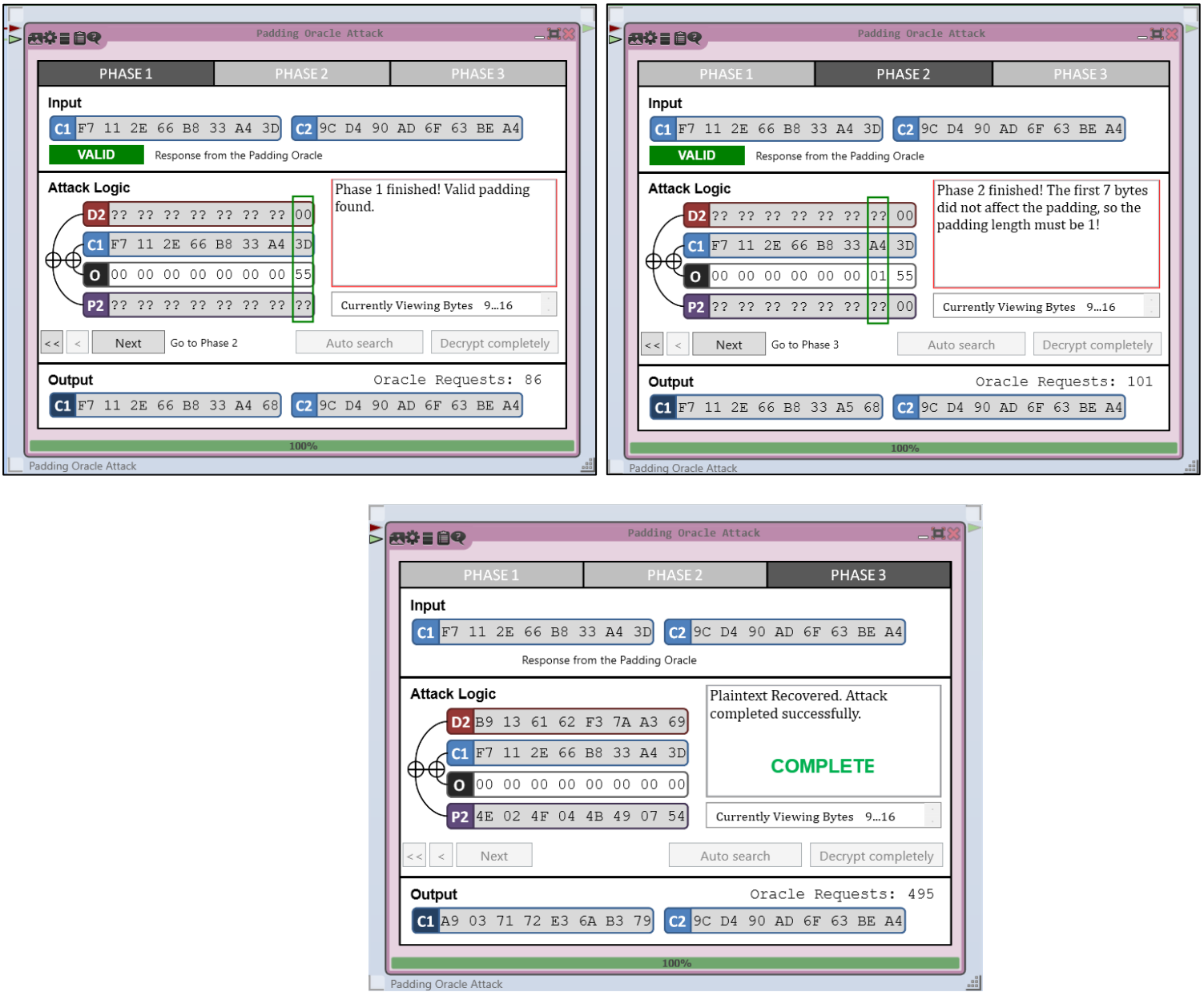
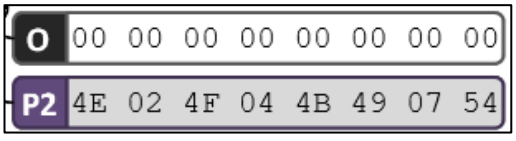


Рисунок 17 – выполнение 3х фаз атаки

5. Убедитесь, что атака удалась.



Выводы.

- Изучен демонстрационный пример шифра AES. Шифр AES использует структуру «Квадрат». На вход получает блок текста размером 128 бит и ключ (128, 192, 256 бит) в шестнадцатеричной системе счисления. Каждый раунд, за исключением последнего, состоит из 4 слоев: подстановки, перемешивание строк, перемешивание столбцов, XOR с раундовым ключом.
- Произведен расчет преобразований для первого раунда и первого раундового ключа. При проверке результатов с помощью приложения-инспектора расчеты совпали.
- Проведен анализ финалистов конкурса AES. По результатам видно, что значения энтропии для каждого из 5 шифров примерно одинаковы и заметно выше, чем у исходного текста, что говорит о надежности шифра. Наибольшее значение (6.13) получено при использовании Twofish. Все шифры показали почти одинаковое время расшифровки при известной части ключа от 10 байт, что говорит о хорошей криптостойкости шифров. По соотношению энтропии и времени атаки самый эффективный шифр – Twofish.
- Проведена атака «грубой силой» на шифр. Временные затраты на дешифовку с использованием максимального количества ядер (8) составили 1157 дней, что означает высокую криптостойкость шифра. Выявлено, что с увеличением количества ядер уменьшается время на дешифровку. Проведение атаки со знанием части открытого текста и использованием его в качестве оценочной функции ускоряет процесс дешифровки примерно в 2 раза. Так, при знании 12 байт ключа и использовании 3 ядер время уменьшается с 52 минут до 25.
- Проведена атака на шифротекст методом Padding Oracle Attack. По изображениям видно, что атака прошла успешно и второй блок исходного текста был правильно дешифрован. Более того, произошло 495 обращений к серверу из возможных 4080, что в разы меньше, чем атака «грубой силой».