**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

|  |  |  |
| --- | --- | --- |
| Студентка гр. 8383 |  | Гречко В.Д. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

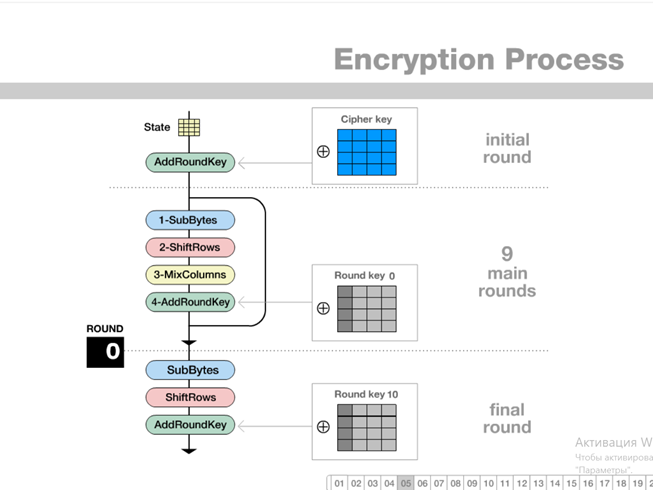
**Цель работы.**

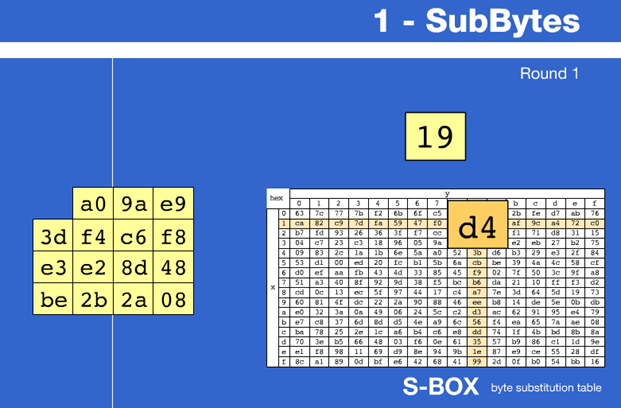
Исследовать характеристики шифра AES и финалистов конкурса AES, а также изучить атаку предсказанием дополнения и получить практические навыки работы с шифрами и проведения атаки, в том числе с использованием приложения Cryptool 1 и 2.

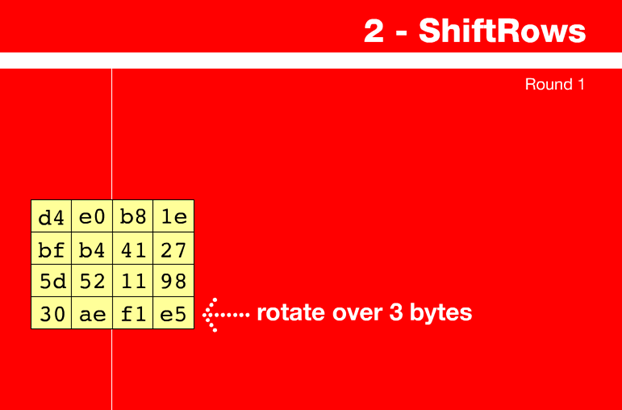
**Исследование преобразований AES.**

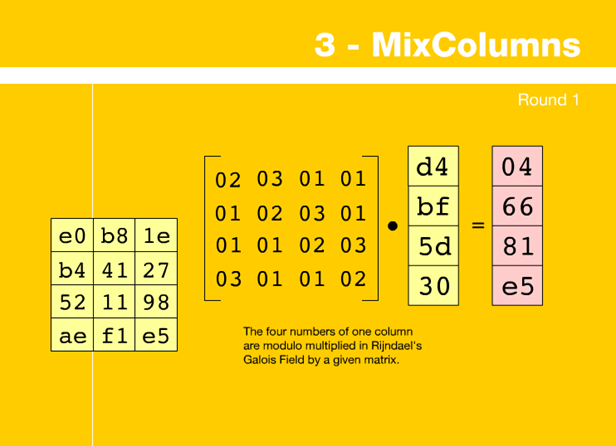
Задание.

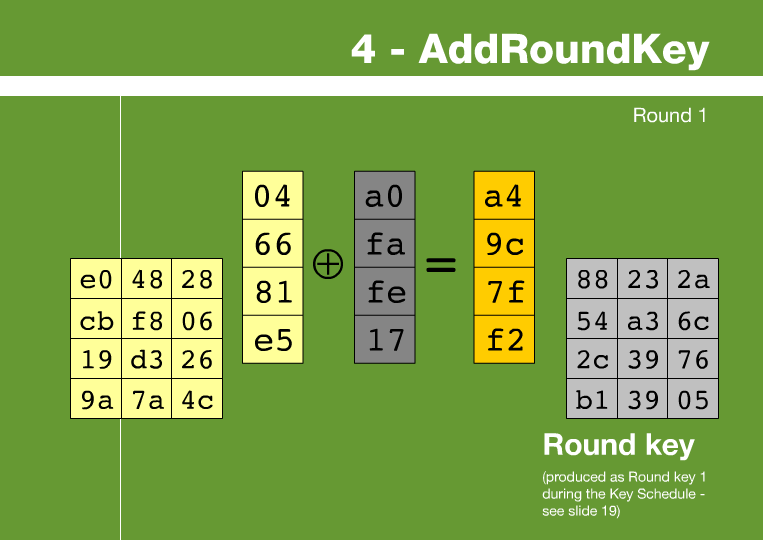
1. Изучить преобразования шифра AES с помощью демонстрационного приложения из Cryptool 1: Indiv.Procedures->Visualization…->AES->Rijndael Animation.

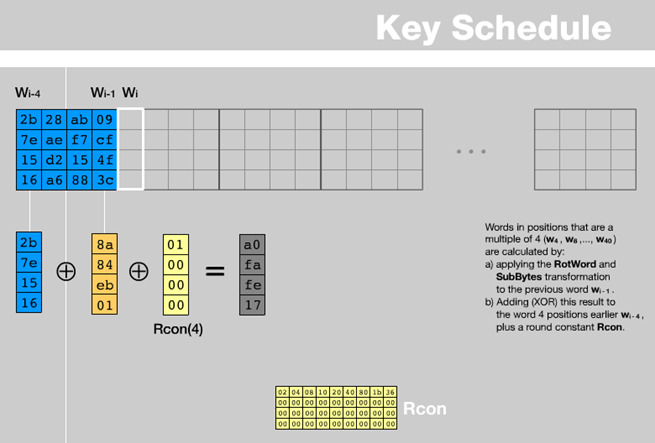


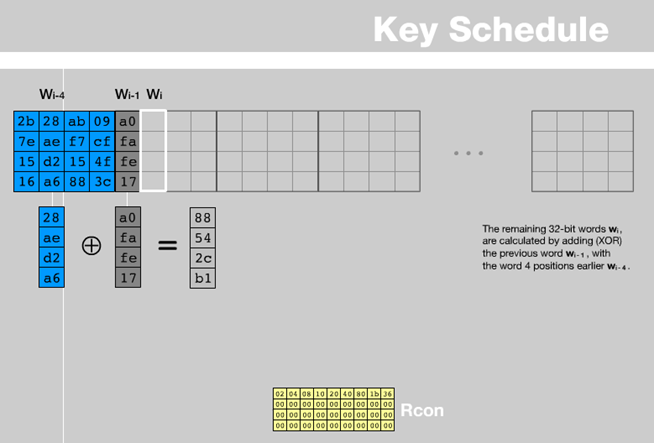






****

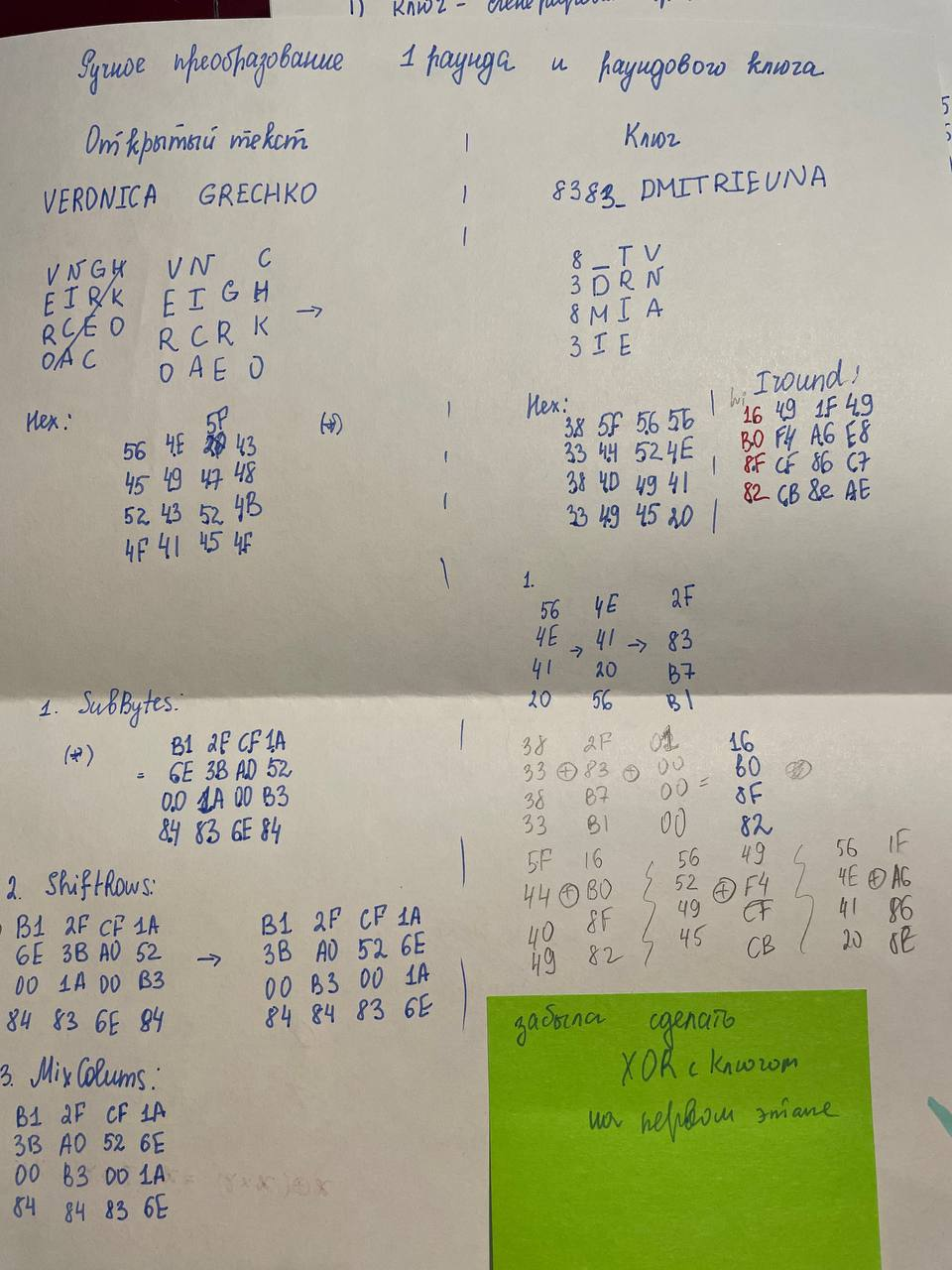


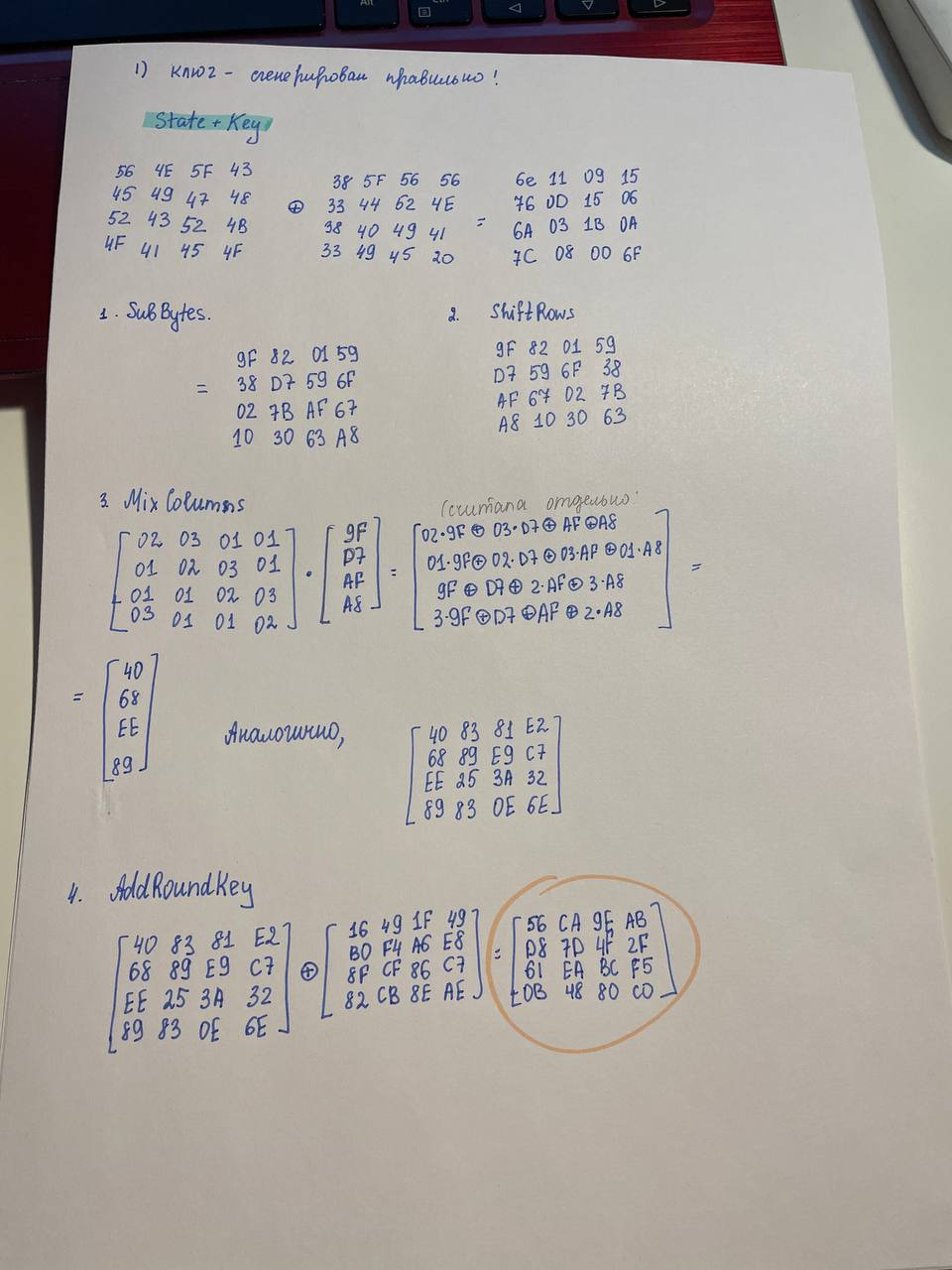


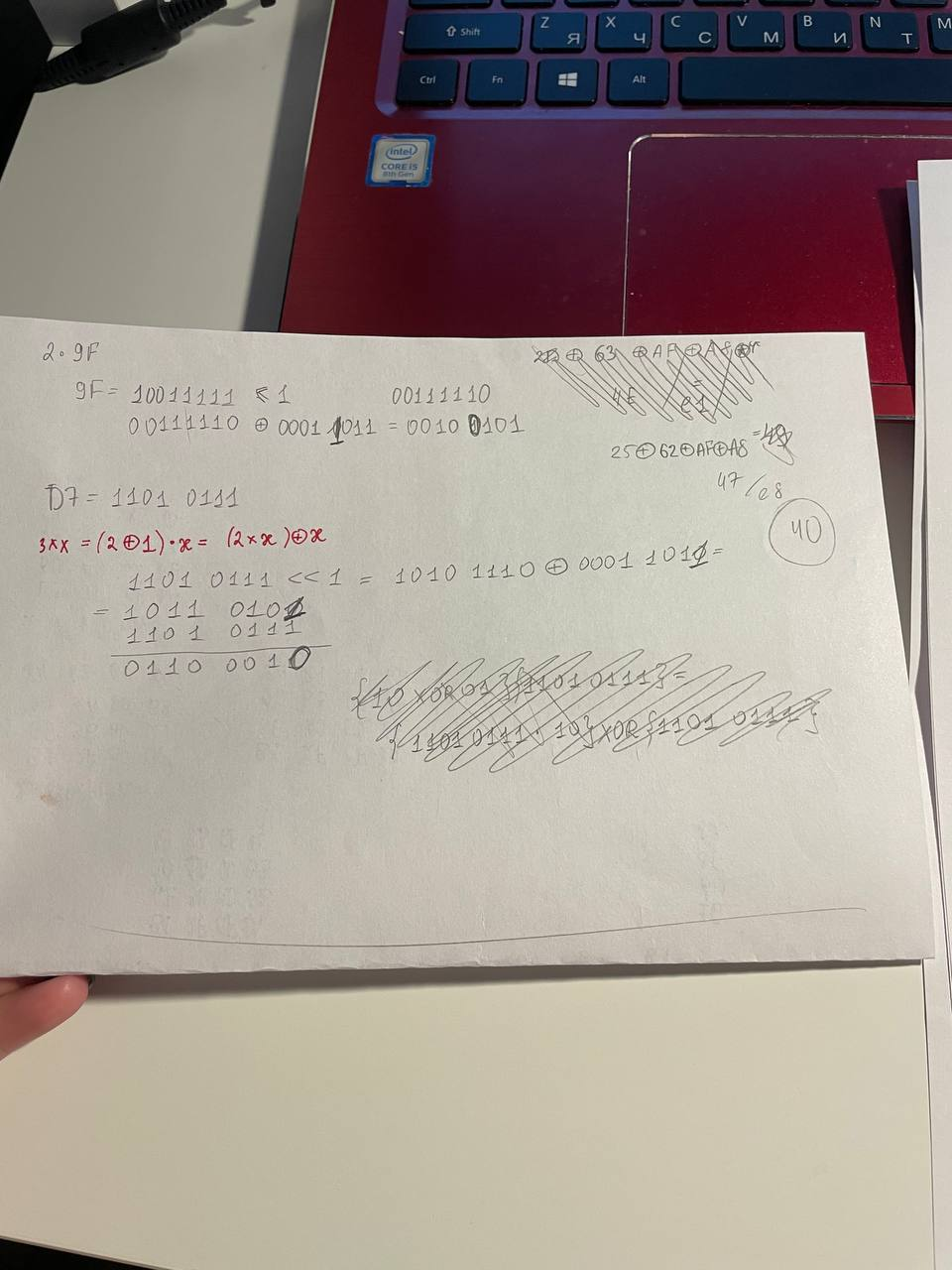
*Рисунок 1 – Запуск демонстрационного примера*

1. Выполнить вручную преобразования для одного раунда и вычисление раундового ключа при следующих исходных данных:
   1. Открытый текст – фамилия\_имя (транслитерация латиницей)
   2. 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*

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

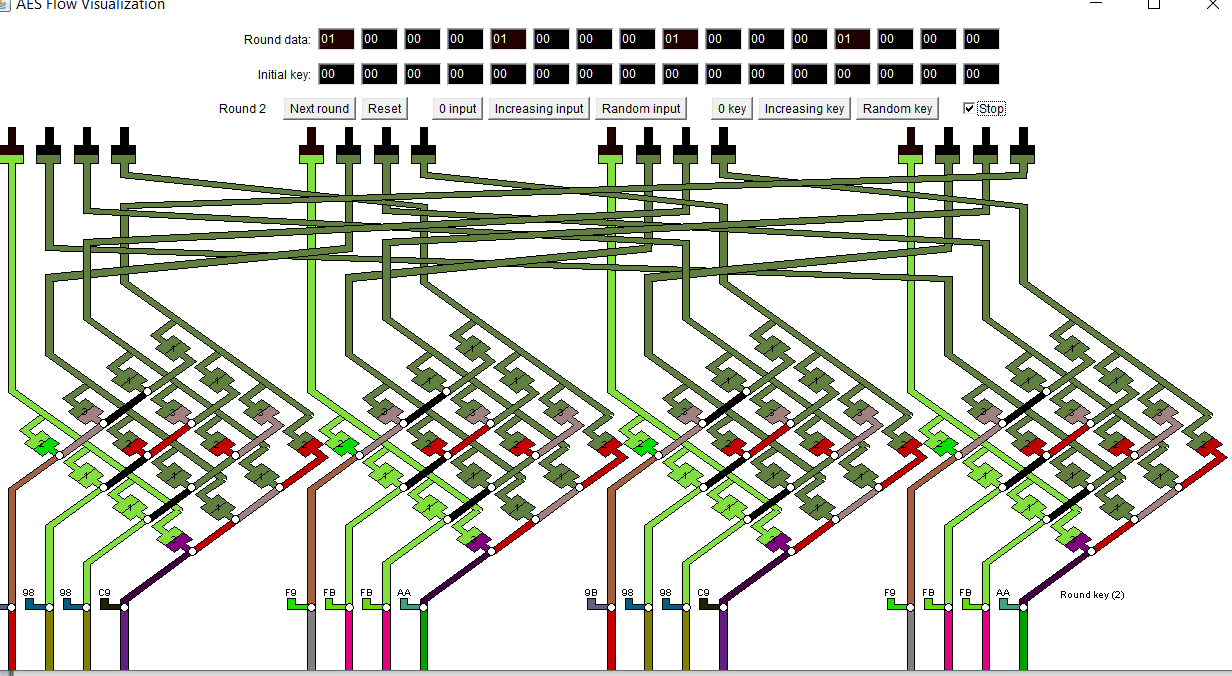
Была выполнена проверка ручных расчетов через CrypTool. Из рис. 3 видно, что результаты совпали.



*Рисунок 3 – Раундовое шифрование AES в CrypTool*

1. 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.



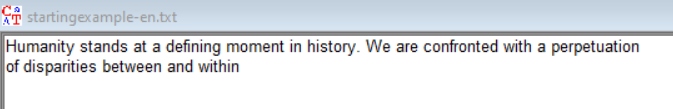
*Рисунок 4 – Rijndael Flow Visualisation для 0-текста и 0-ключа*

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

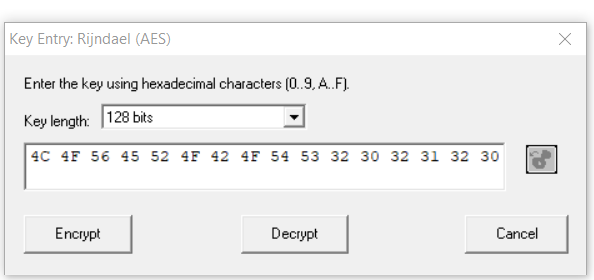
Задание.

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. Исходный ключ представлен на рис. 6.



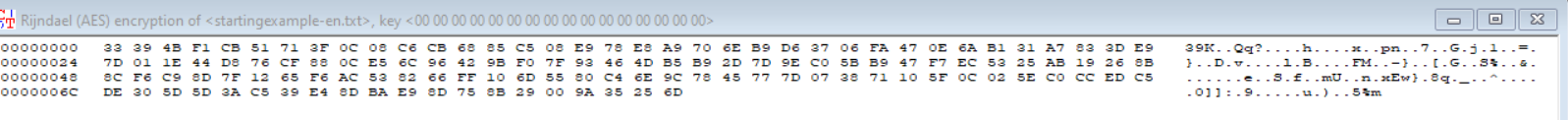
*Рисунок 5 – Исходный текст*



*Рисунок 6 – Исходный ключ*

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

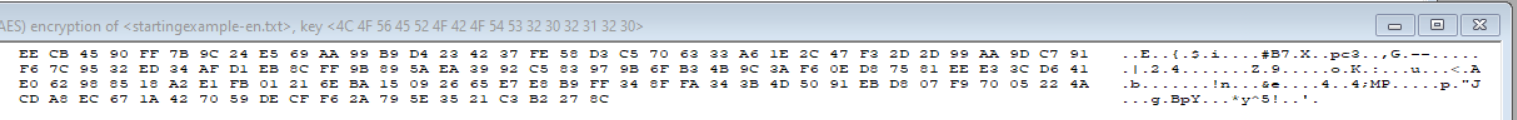
Было выполнено шифрование исходного текста с 0-ключом. Результат представлен на рис.7.



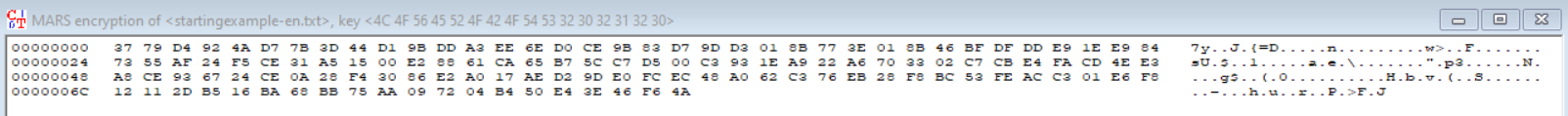
*Рисунок 7 – Шифрование с 0-ключом*

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

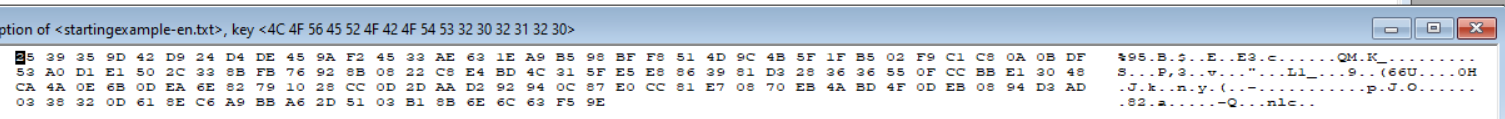
Было выполнено шифрование исходного текста с выбранным ключом (рис. 6) шифрами AES, MARS, RC6, Serpent и Twofish. Результаты представлены на рис. 8 – 12 соответственно.



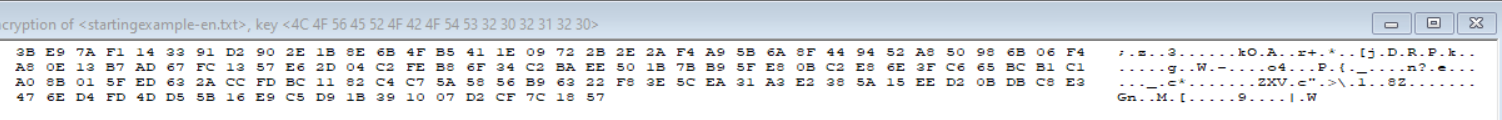
*Рисунок 8 – Результат работы шифра AES*



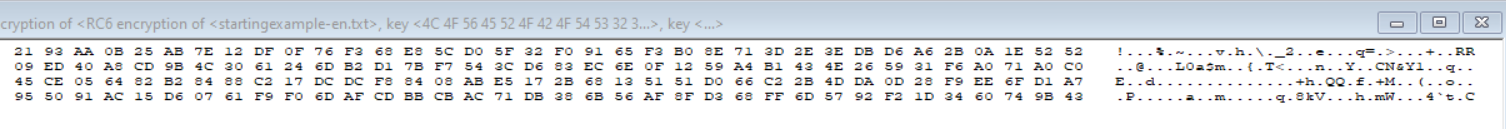
*Рисунок 9 – Результат работы шифра MARS*



*Рисунок 10 – Результат работы шифра RC6*



*Рисунок 11 – Результат работы шифра Serpent*



*Рисунок 11 – Результат работы шифра Twofish*

1. 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 |  |
| AES |  |
| MARS |  |
| RC6 |  |
| Serpent |  |
| Twofish |  |

1. 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*

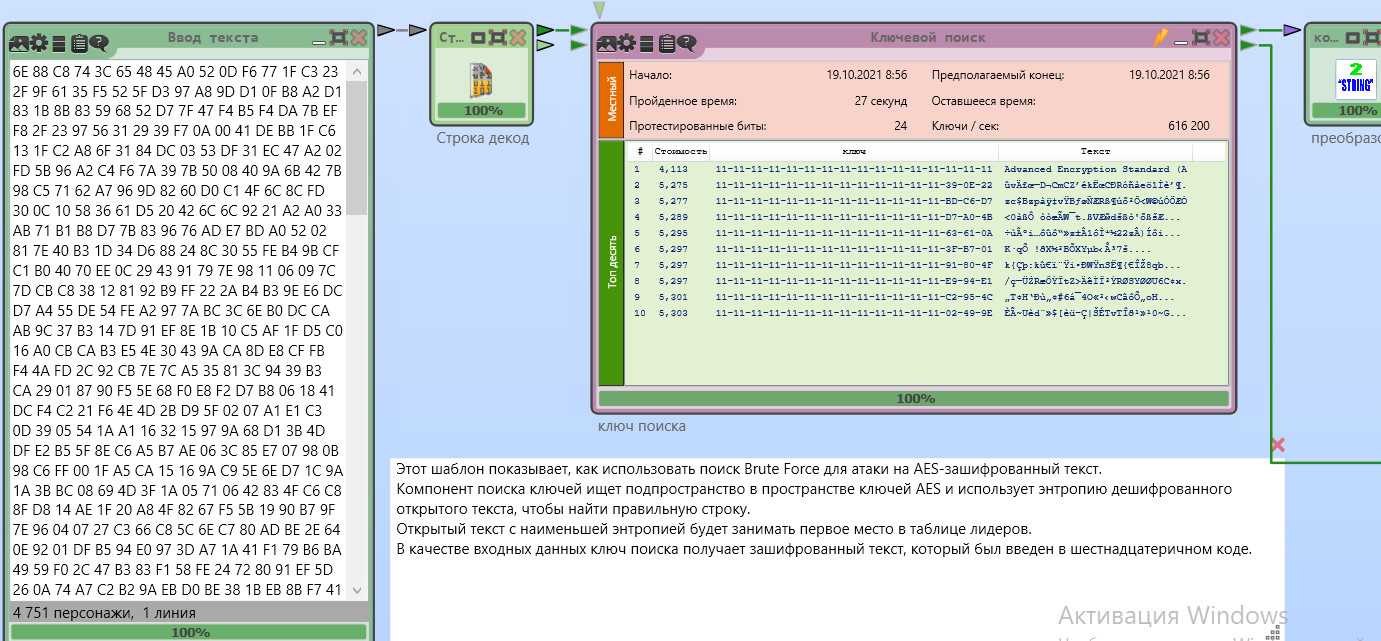
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Количество известных байт | AES | MARS | RC6 | Serpent | Twofish |
| 14 | менее секунды | менее секунды | менее секунды | менее секунды | менее секунды |
| 13 | 20 сек | 34 сек | 20 сек | 1 мин | 38 сек |
| 12 | часа | час | часа | 4 часа | 3 часа |
| 11 | 18 дней | 27 дней | 17 дней | 48 дней | 34 дней |
| 10 | 12 лет | 19 лет | 11 лет | 35 лет | 21 год |
| 9 | лет | лет | лет | лет | лет |
| 8 | лет | лет | лет | лет | лет |
| 6 | лет | лет | лет | лет | лет |
| 4 | лет | лет | лет | лет | лет |
| 2 | лет | лет | лет | лет | лет |

**Атака «грубой силы» на AES.**

Задание.

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

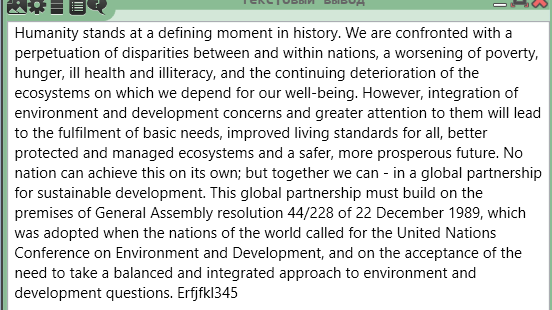
Был изучен шаблон атаки на шифр AES с использованием энтропии. Шаблон представлен на рис. 12.



*Рисунок 12 – Шаблон атаки AES Analysis using Entropy*

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

Исходный текст представлен на рис. 13. Ключ представлен на рис. 6.



*Рисунок 13 – Исходный текст*

1. 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.

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

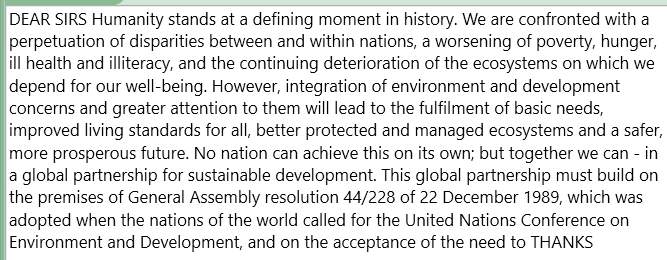
Установим требуемые параметры в программе и исследуем затраты времени. Результаты сведем в таблицу 3.

*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 | 2 секунды | 2 секунды | 2 секунды | 2 секунды |
| 12 | 1 час 40 минут | 36 минут | 26 минут | 20 минут |
| 10 | 4976 дней | 1659 дней | 976 дней | 789 дней |

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

Результат нового исходного текста представлен на рис. 14.



*Рисунок 14 – Исходный текст*

1. 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.

1. 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»*

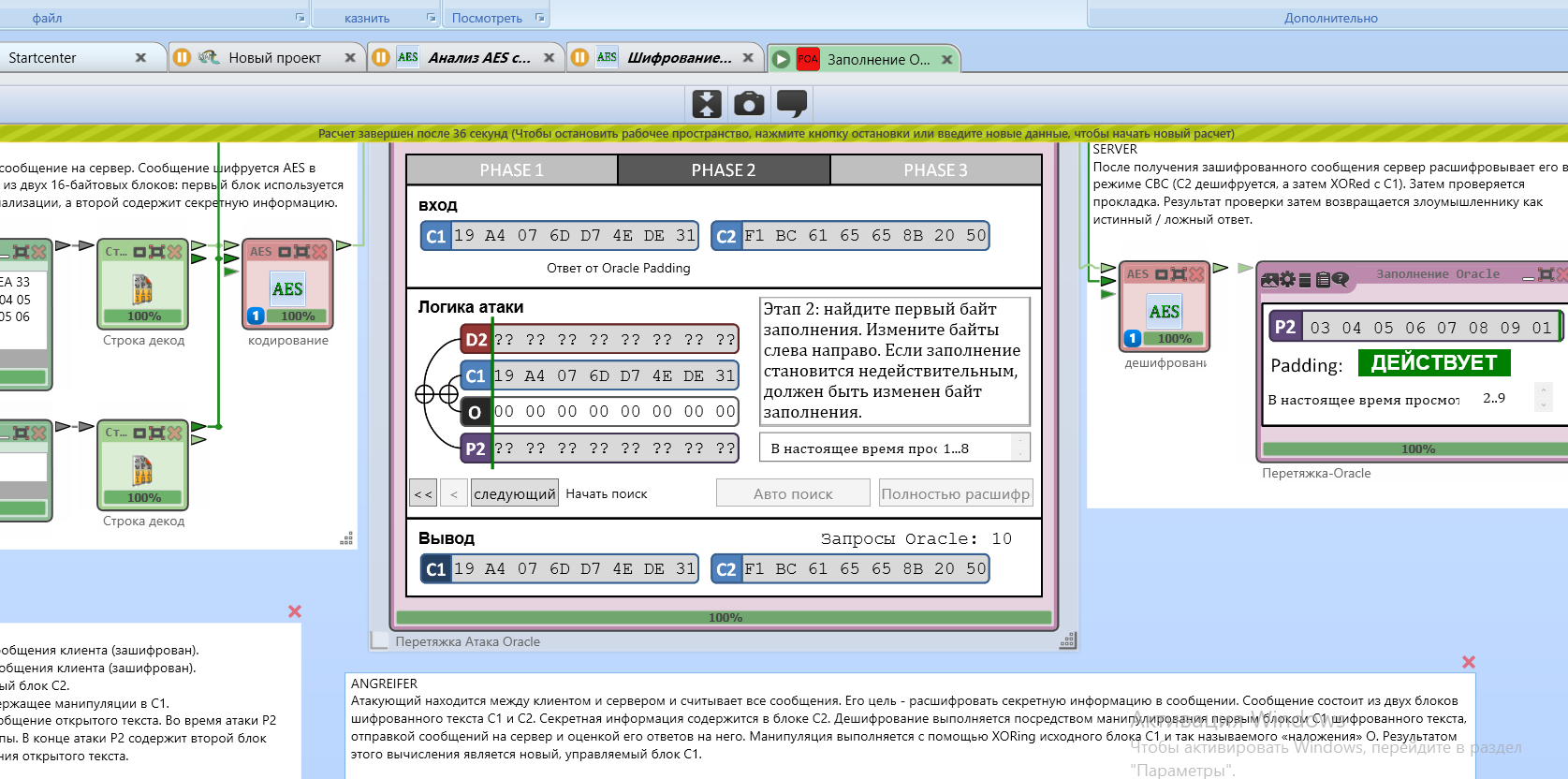
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Известная часть ключа, байт | Время атаки грубой силы | | | |
| Количество ядер | | | |
| 1 | 3 | 6 | 8 |
| 14 | 2 секунды | 2 секунды | 2 секунды | 2 секунды |
| 12 | 20 минут | 10 минут | 6 минут | 6 минут |
| 10 | 922 день | 386 дней | 315 дней | 297 дней |

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

Задание.

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*

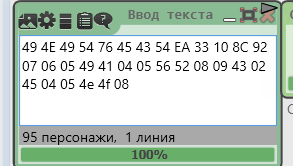
1. Подготовьтесь к атаке теоретически:

a. Изучите комментарии к шаблону

b. Изучите публикацию [4]

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

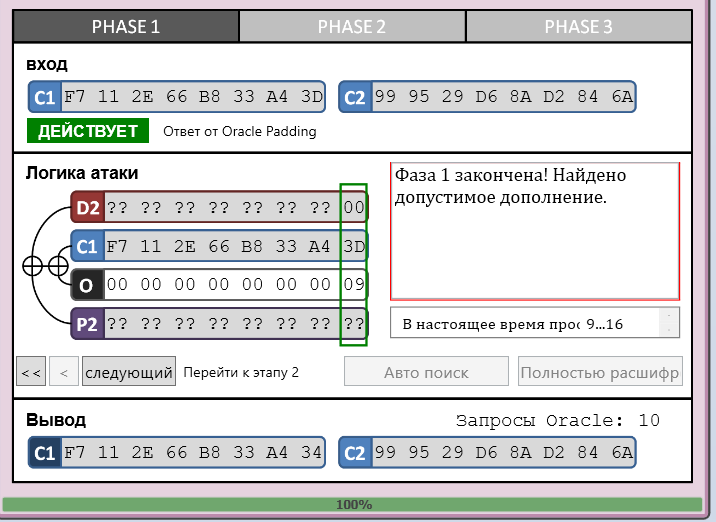
Результат изменения исходного текста представлен на рис. 16.

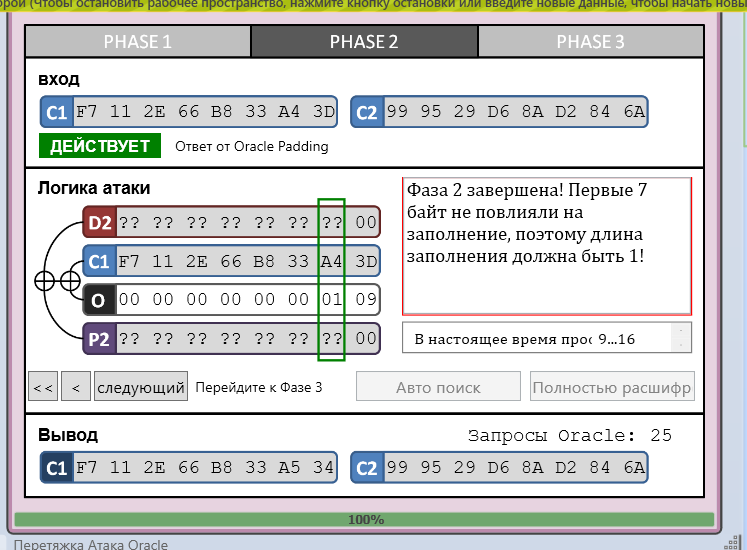


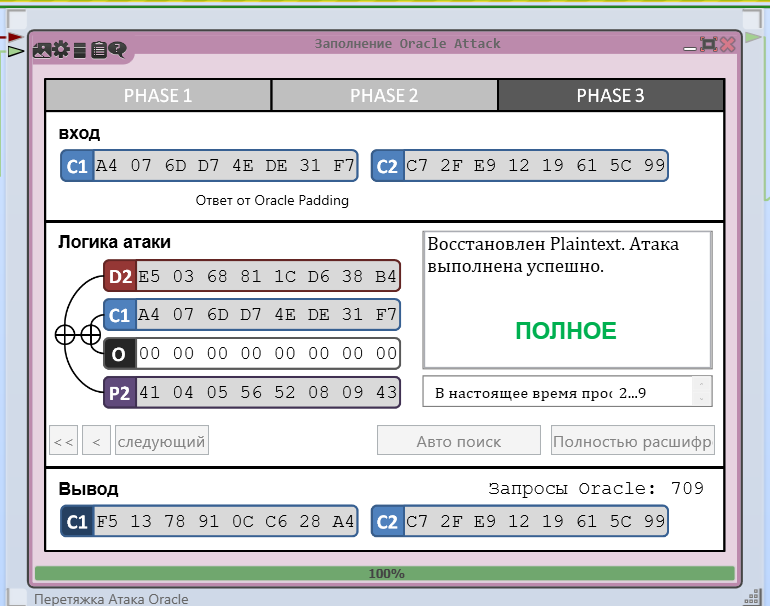
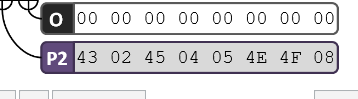
*Рисунок 16 – Изменённый исходный текст*

1. 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*

1. Убедитесь, что атака удалась.

**Выводы.**

1. Изучен демонстрационный пример шифра AES. Шифр AES использует структуру «Квадрат». На вход получает блок текста размером 128 бит и ключ (может быть 128, 192 или 256 бит) в шестнадцатеричной системе счисления. Каждый раунд за исключением последнего состоит из 4 слоев: подстановки, перемешивание строк, перемешивание столбцов, XOR с раундовым ключом для противодействия линейному и дифференциальному криптоанализу.
2. Был проведен анализ финалистов конкурса AES. По результатам таблицы 1 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 (6.65) получено при использовании RC6 и Twofish. Все шифры показали почти одинаковое время расшифровки при известной части ключа от 9 байт, что говорит о хорошей криптостойкости шифров. Однако, шифр Serpent показал наилучший результат даже при большой известной части ключа – 4 часа при 12 байтах. По соотношению энтропии и времени атаки самый эффективный шифр – Twofish.
3. Проведение атаки «грубой силой» в первом случае продемонстрировало, что знание даже 10 байт секретного ключа не ускоряет процесс дешифровки. Временные затраты на дешифовку с использованием максимального количества ядер (в данном случае 8) составили 789 дней, что означает высокую криптостойкость шифра. Выявлено, что с увеличением количества ядер заметно уменьшается время на дешифровку, и данной аппаратной характеристикой не стоит пренебрегать при проведении атаки. Проведение атаки со знанием части открытого текста и использованием его в качестве оценочной функции ускоряет процесс дешифровки в 3-5 раз, что демонстрирует одну из серьёзных уязвимостей шифра. Так, при знании 12 байт ключа и использовании 6 ядер время уменьшается с 26 минут до 6. Более того, такая атака работает хорошо даже при использовании не максимального количества ядер – затраты времени практически идентичны как для 8 ядер, так и для 6.
4. Была проведена атака на шифротекст методом Padding Oracle Attack. По последним изображениям видно, что атака прошла успешно и мы дешифровали второй блок исходного текста верно. Более того, произошло 709 обращений к серверу из возможных 4080, что в разы меньше, чем атака «грубой силой».