**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №5**

**по дисциплине «Криптографические методы защиты информации»**

**Тема: Изучение шифра AES**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 4383 |  | Гордеева Т.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2017

**Цель работы:** исследовать шифр AES, финалистов конкурса AES, атаку предсказанием дополнения и получить практические навыки работы с шифрами и атакой, в том числе и в программном продукте Cryptool 1 и 2.

**1 Исследование преобразований AES**

**1.1 Задание**

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

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

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

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

**1.2 Содержание раздела отчета**

1. Формулировка задания.

2. Описание AES c примерами скриншотов из демоприложения.

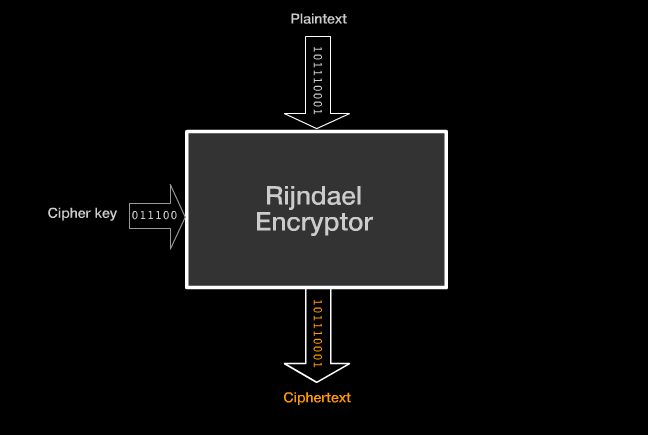
3. Расчет матрицы состояний и раундового ключа шифра для одного раунда.

4. Скриншоты приложения-инспектора, подтверждающие корректность расчетов.

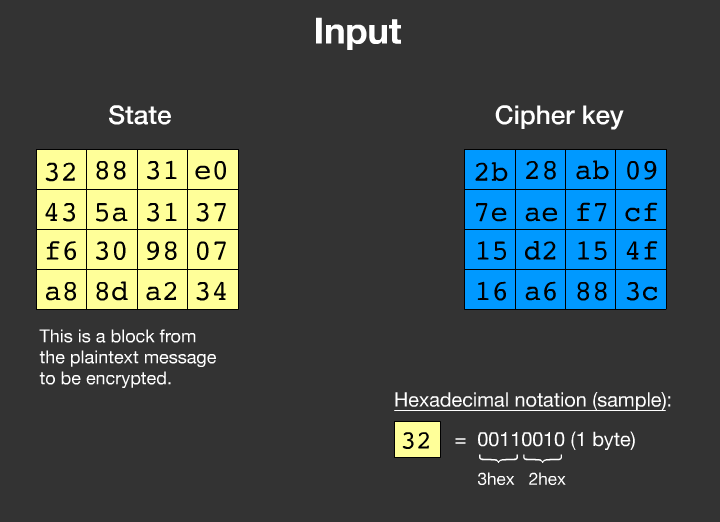
5. Выводы.

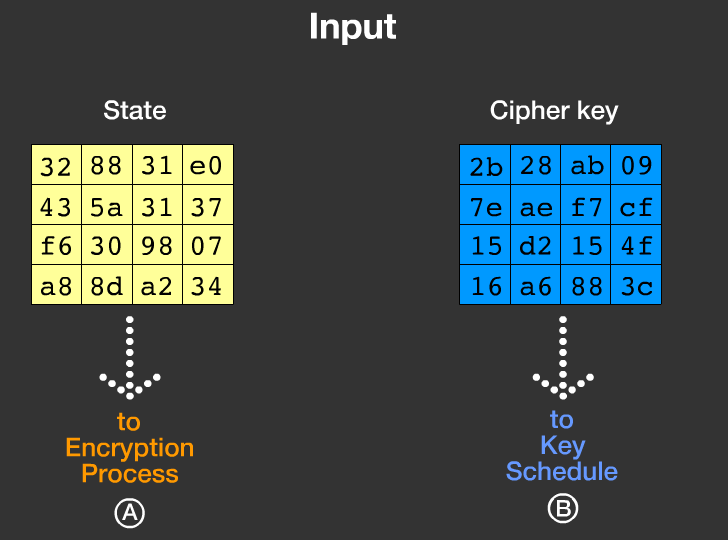
**1.3 Описание AES c примерами скриншотов из демоприложения.**

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

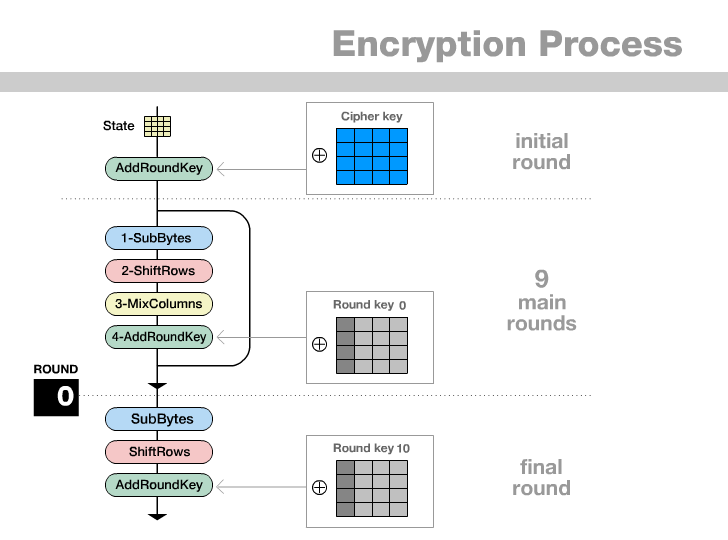
****

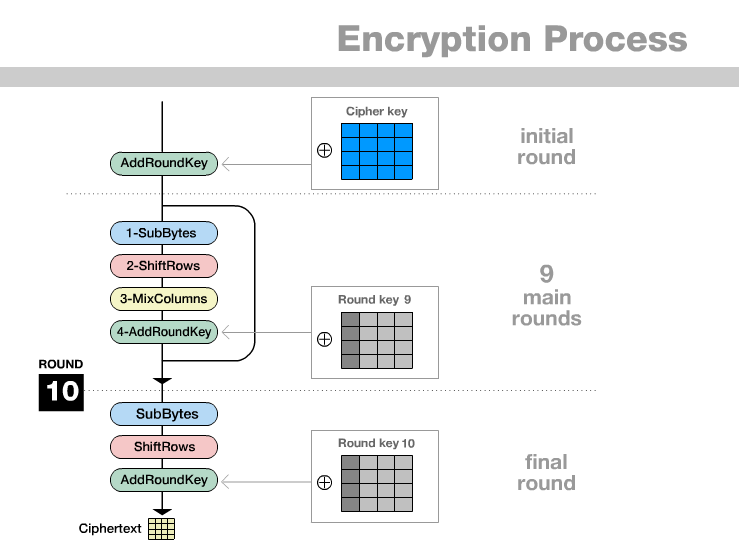
Входные данные:

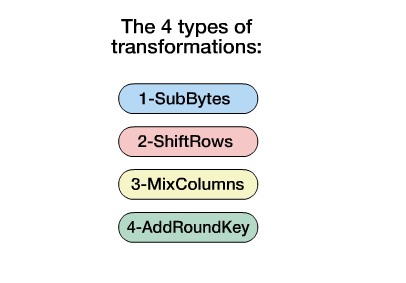
****

****

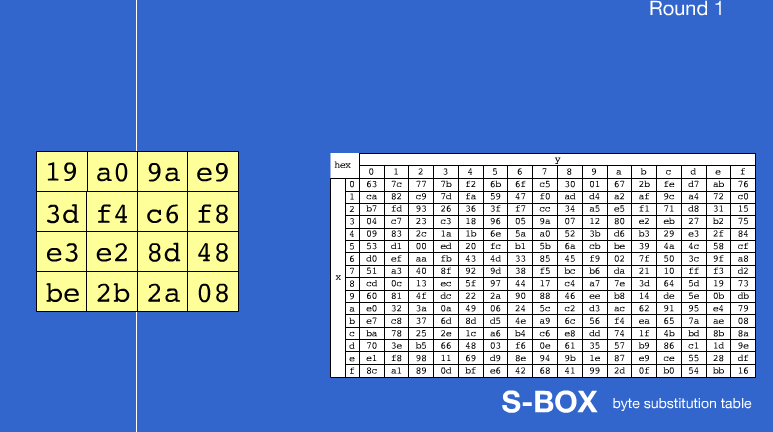
Процесс шифрования состоит из 10 раундов:

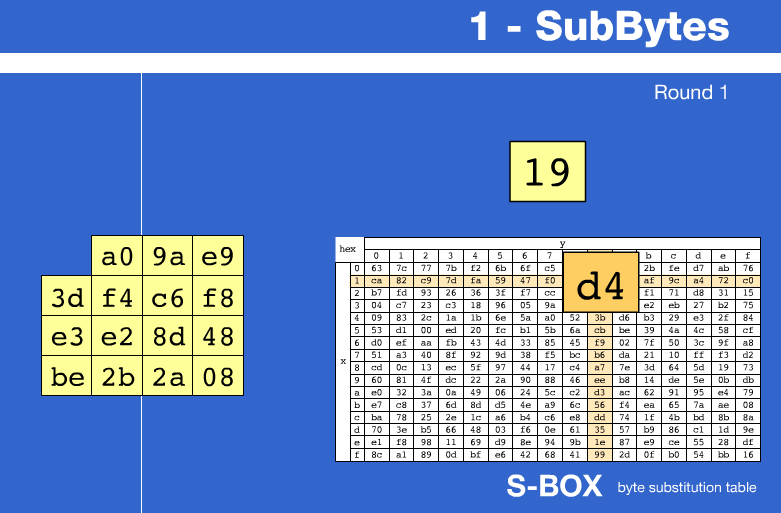
****

****

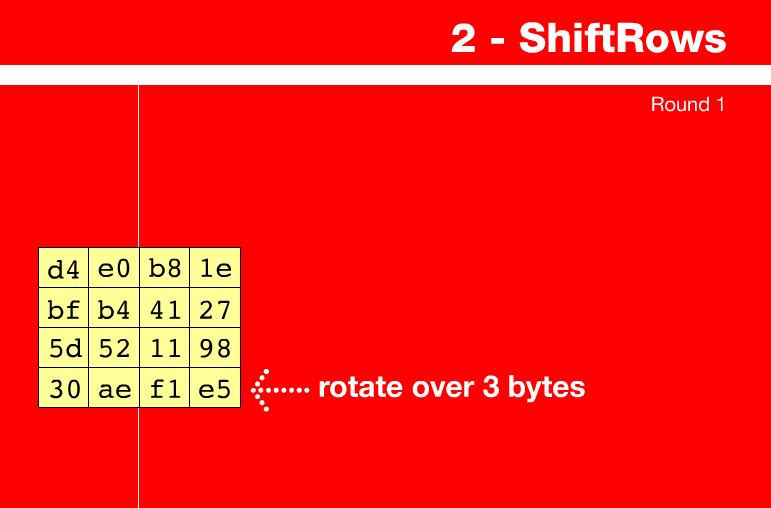
****

Использование преобразования подстановки SubBytes.

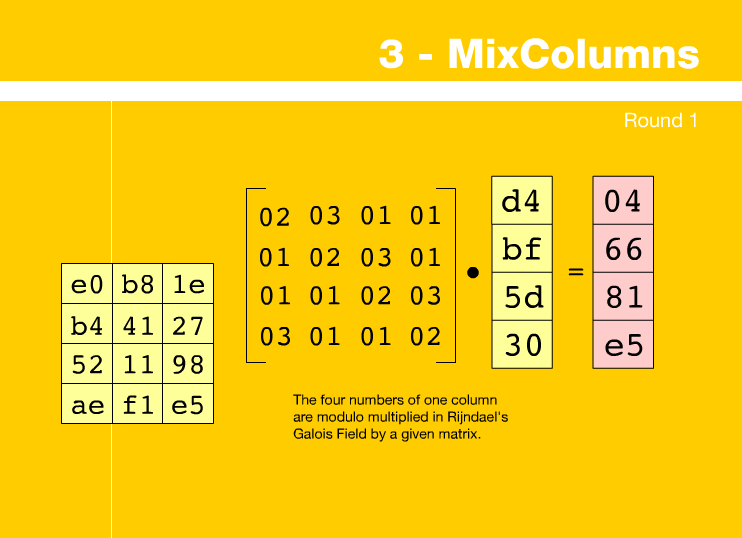
****

****

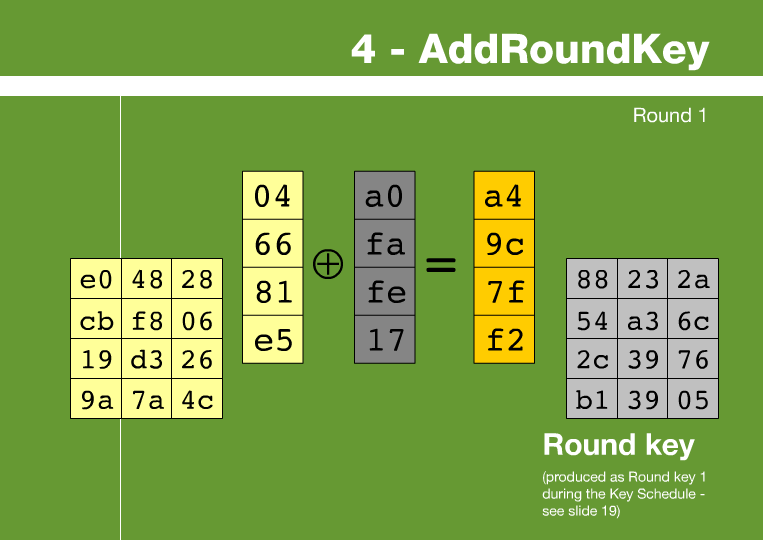
Циклический сдвиг влево всех строк матрицы состояний преобразованием ShiftRows.

****

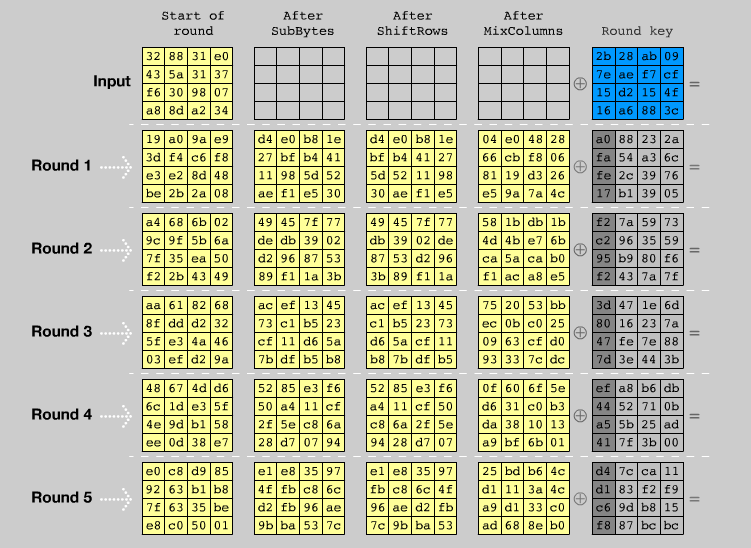
Смешивание столбцов матрицы состояний путем ее умножения на матрицу констант в конечном поле 𝐺𝐹(28– преобразовние MixColumns.

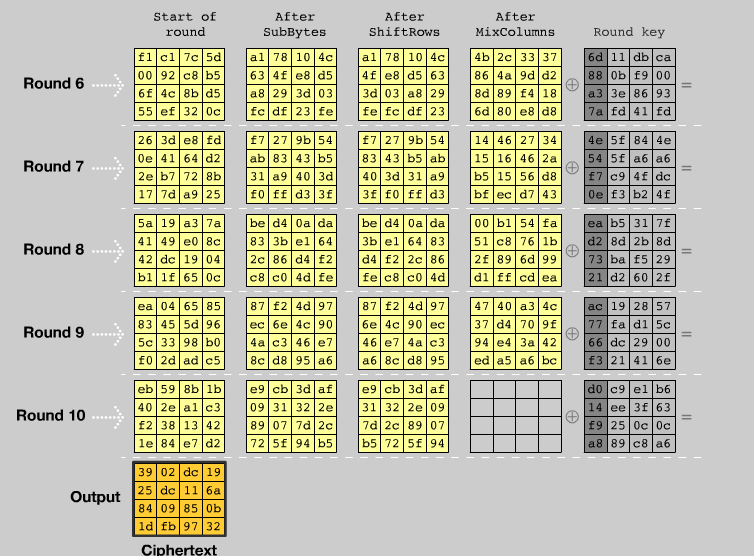
****

Сложение полученных столбцов матрицы состояний с раундовым ключом операцией xor – преобразование AddRoundKey

****

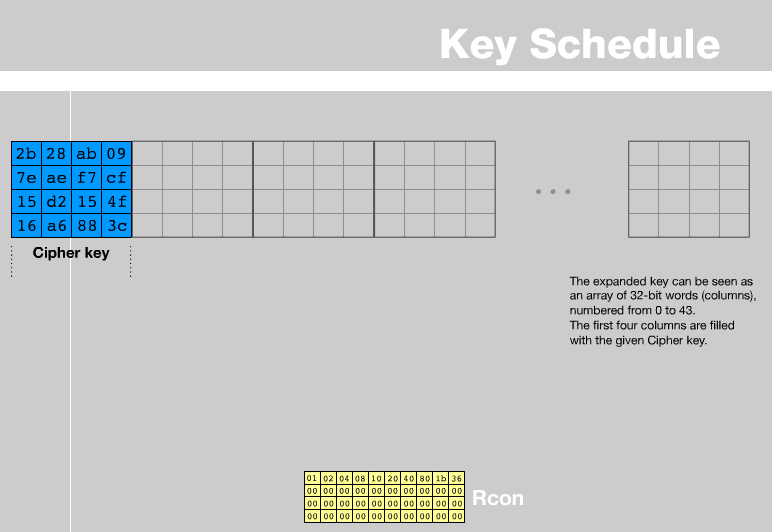
Повторение операций на каждом из 10 раундов.

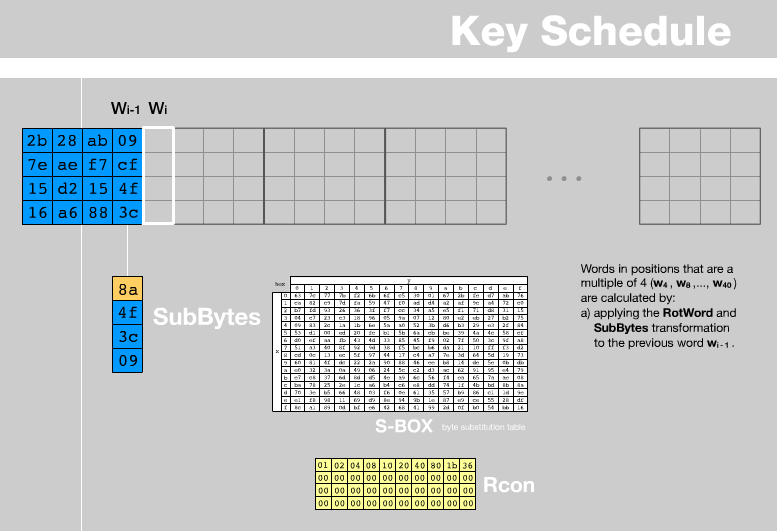
****

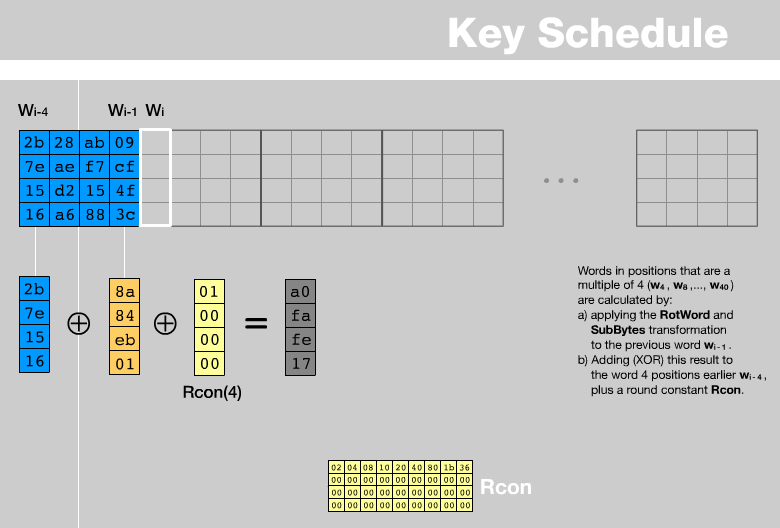
****

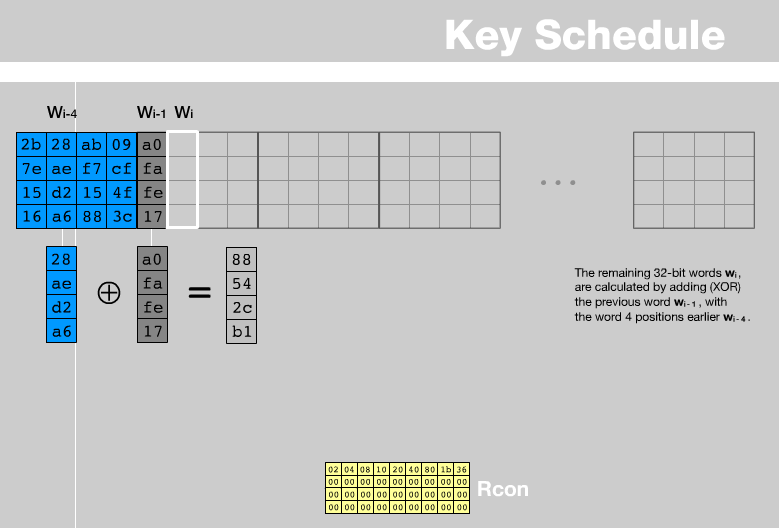
Последний раунд не включает в себя смешивание столбцов.

Генерация раундовых ключей:

****

****

****

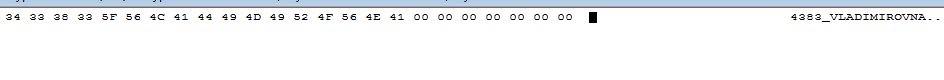
****

**1.4 Расчет матрицы состояний и раундового ключа шифра для одного раунда.**

Открытый текст:



Ключ:



Открытый текст:

|  |  |  |  |
| --- | --- | --- | --- |
| 54 | 41 | 42 | 56 |
| 41 | 5F | 44 | 41 |
| 4E | 47 | 45 | 0 |
| 59 | 4F | 45 | 0 |

Ключ:

|  |  |  |  |
| --- | --- | --- | --- |
| 34 | 5F | 44 | 52 |
| 33 | 56 | 49 | 4F |
| 38 | 4C | 4D | 56 |
| 33 | 41 | 49 | 4E |

1. Подготовка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 54 | 41 | 42 | 56 | xor | 34 | 5F | 44 | 52 | = | 60 | 1E | 16 | 04 |
| 41 | 5F | 44 | 41 | 33 | 56 | 49 | 4F | 72 | 09 | 0d | 0e |
| 4E | 47 | 45 | 0 | 38 | 4C | 4D | 56 | 76 | 0b | 08 | 56 |
| 59 | 4F | 45 | 0 | 33 | 41 | 49 | 4E | 6a | 0e | 0c | 4e |

2. Преобразование подстановки SubBytes

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 60 | 1E | 16 | 04 | (S-box)  = | d0 | 72 | 47 | f2 |
| 72 | 09 | 0d | 0e | 40 | 01 | d7 | ab |
| 76 | 0b | 08 | 56 | 38 | 2b | 30 | b1 |
| 6a | 0e | 0c | 4e | 02 | ab | fe | 2f |

3. Преобразование ShiftRows

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d0 | 72 | 47 | f2 | (S-box)  = | d0 | 72 | 47 | f2 |
| 40 | 01 | d7 | ab | 01 | d7 | ab | 40 |
| 38 | 2b | 30 | b1 | 30 | b1 | 38 | 2b |
| 02 | ab | fe | 2f | 2f | 02 | ab | fe |

4. Преобразование MixColumns

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d0 | 72 | 47 | f2 | Умножение каждого столбца в поле GF(28) | 02 | 03 | 01 | 01 | = | a7 | 35 | fb | ea |
| 01 | d7 | ab | 40 | 01 | 02 | 03 | 01 | ad | 0d | e9 | f1 |
| 30 | b1 | 38 | 2b | 01 | 01 | 02 | 03 | c0 | da | 7a | fd |
| 2f | 02 | ab | fe | 03 | 01 | 01 | 02 | 04 | f4 | 17 | 81 |

5. Г5. Генерация раундовых ключей:

|  |  |  |  |
| --- | --- | --- | --- |
| 34 | 5F | 44 | 52 |
| 33 | 56 | 49 | 4F |
| 38 | 4C | 4D | 56 |
| 33 | 41 | 49 | 4E |

Матрица Rcon

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1b | 36 |
| 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

wi

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 34 | 5F | 44 | 52 | b1 | ee | aa | f8 |
| 33 | 56 | 49 | 4F | 82 | d4 | 9d | d2 |
| 38 | 4C | 4D | 56 | 17 | 5b | 16 | 40 |
| 33 | 41 | 49 | 4E | 33 | 72 | 3b | 75 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 34 | xor | 84 | xor | 01 | = | b1 |
| 33 | b1 | 00 | 82 |
| 38 | 2f | 00 | 17 |
| 33 | 00 | 00 | 33 |

wi=

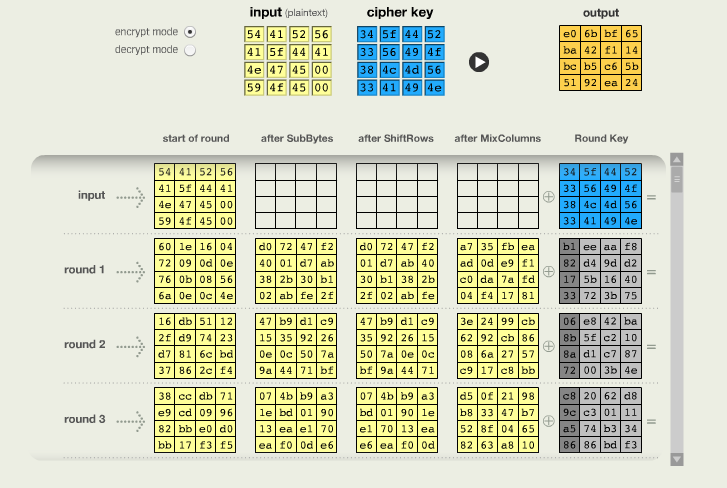
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5F | xor | b1 | = | ee |
| 56 | 82 | d4 |
| 4C | 17 | 5b |
| 41 | 33 | 72 |

wi+1=

6. Результат первого раунда:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a7 | 35 | fb | ea | xor | b1 | ee | aa | f8 | = | b1 | ee | aa | f8 |
| ad | 0d | e9 | f1 | 82 | d4 | 9d | d2 | 82 | d4 | 94 | d2 |
| c0 | da | 7a | fd | 17 | 5b | 16 | 40 | 17 | 5b | 16 | 40 |
| 04 | f4 | 17 | 81 | 33 | 72 | 3b | 75 | 33 | 72 | 3b | 75 |

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

****

**1.5 Выводы.**

В ходе выполнения данного пункта была изучена схема работы алгоритма AES. После изучения алгоритма с помощью демонстрационного приложения из CrypTool 1 были произведены расчет преобразований для первого раунда и первого раундового ключа. При проверке результатов с помощью приложения-инспектора расчеты совпали.

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

**2.1 Задание**

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

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

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

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

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.

**2.2 Содержание раздела отчета**

1. Формулировка задания.

2. Исходные данные для экспериментов:

a. Исходный текст

b. Секретный ключ

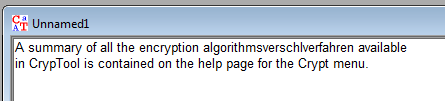
3. Таблица с результатами качества зашифрования исследованными шифрами.

4. Таблица с результатами трудоемкости атаки «грубой силы» для исследованных шифров.

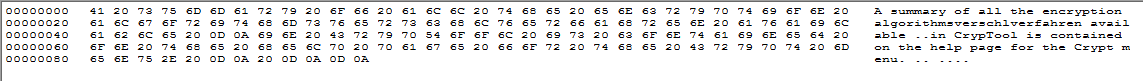
5. Выводы.

**2.3 Исходные данные для экспериментов**

Исходный текст:

****

Бинарный файл:



Секретный ключ:

12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

**2.4 Таблица с результатами качества зашифрования исследованными шифрами.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Исходный текст | AES | MARS | RC6 | Serpent | Twofish |
| Энтропия | 4,33 | 6,68 | 6,59 | 6,68 | 6,69 | 6,62 |

**2.5 Таблица с результатами трудоемкости атаки «грубой силы» для исследованных шифров.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Количество известных байт | AES | MARS | RC6 | Serpent | Twofish |
| 14 | менее секунды | менее секунды | менее секунды | менее секунды | менее секунды |
| 13 | 36 секунд | 50 секунды | 34 секунды | 1 час 36 минут | 55 секунд |
| 12 | 2часа 36 минут | 2 часа 27 минут | 2 часа 27 минут | 7 часов | 4 часа |
| 11 | 25,8 дней | 42,2 дня | 25,3 дня | 73,5 дня | 43,7 дня |
| 10 | 19 лет | 29 лет | 19 лет | 51 год | 31 год |
| 9 | 4900 лет | 7400 лет | 4500 лет | 1,3\*104 лет | 7800 лет |
| 8 | 1,2\*106 лет | 1,9\*106 лет | 1,2\*106 лет | 3,5\*106 лет | 2\*106 лет |
| 7 | 3,2\*108 лет | 4,8\*108 лет | 3,1\*108 лет | 8,8\*108 лет | 5,1\*108 лет |
| 6 | 7,8\*1010 лет | 1,3\*1011 лет | 7,7\*1010 лет | 2,3\*1011 лет | 1,3\*1011 лет |
| 5 | 2,4\*1013 лет | 3,2\*1013 лет | 2\*1013 лет | 5,6\*1013 лет | 3,4\*1013 лет |
| 4 | 5,2\*1015 лет | 8,5\*1015 лет | 5,2\*1015 лет | 1,7\*1016 лет | 8,6\*1015 лет |
| 3 | 1,4\*1018 лет | 2,1\*1018 лет | 1,4\*1018 лет | 4\*1018 лет | 2,3\*1018 лет |
| 2 | 3,4\*1020 лет | 5,3\*1020 лет | 3,4\*1020 лет | 9,5\*1020 лет | 5,7\*1020 лет |

**2.6 Вывод.**

В ходе выполнения данного пункта было проведено исследование финалистов конкурса AES. Результаты показали, что наибольшую энтропию имеет шифр Serpent. Также шифр Serpent оказался самым криптоустойчивым из рассмотренных шифров. Наименее устойчивыми к атаке «грубой силы» оказались шифры AES и RC6.

**3 Атака «грубой силы» на AES**

**3.1 Задание**

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

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

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.

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

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

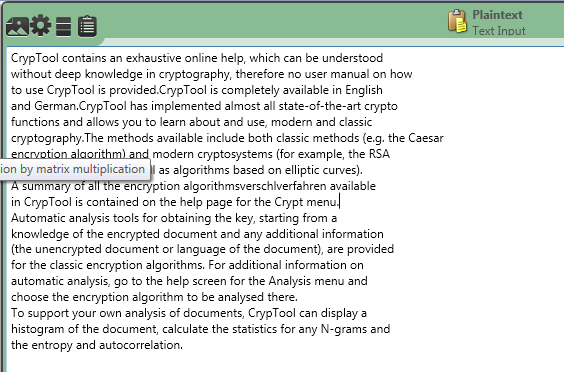
6. Провести атаку «грубой силы» когда известно n-2, n-4, n-6 байт секретного ключа, используя в качестве оценочной функции словосочетание DEAR SIRS задействовав 1 ядро процессора. Зафиксировать затраты времени.

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

**3.2 Исходные данные для экспериментов**

Выберем открытый текст (примерно 1000 знаков) и загрузим его в шаблон.

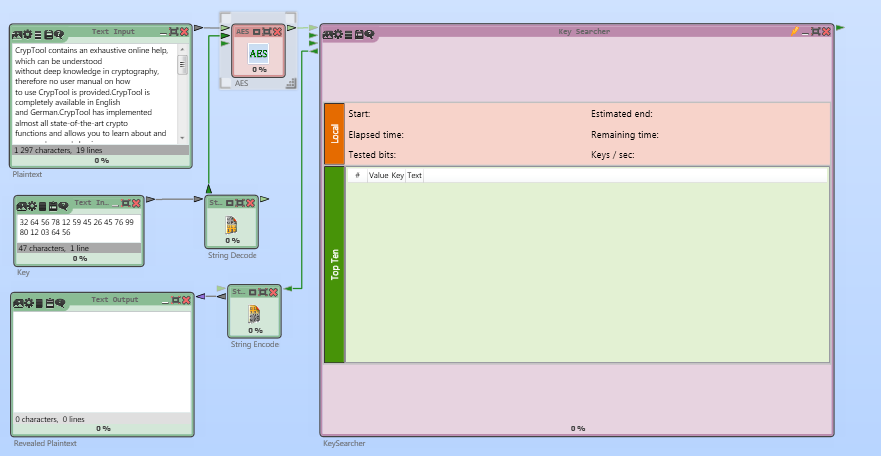
a. Исходный текст



b. Секретный ключ

32 64 56 78 12 59 45 26 45 76 99 80 12 03 64 56

**3.3 Шаблон атаки «грубой силы» из Cryptool 2**

****

**3.4 Таблица с результатами трудоемкости энтропийной атаки «грубойсилы» для различных вариантов знаний о ключе и количестве задействованных процессорных ядер.**

Проведем 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. Зафиксируем затраты времени. Также выполним атаку повторно с средним и максимальным количеством процессорных ядер. Зафиксируем затраты времени.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Известная часть ключа, байт | Время атаки грубой силы | | | |
| Количество ядер | | | |
| 1 | 2 | 3 | 4 |
| 14 | 1 секунда | 1 секунда | 1 секунда | 1 секунда |
| 12 | 2 часа 35 минут | 1 час 30 минут | 1 час 12 минут | 1 час 4 минуты |
| 10 | 7101 день 21 час | 3550 дней 22 часа | 2950 дней 14 часов | 2689 дней 17 часов |

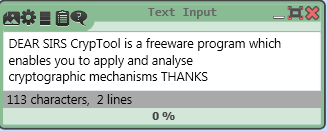
**3.5 . Таблица с результатами трудоемкости текстовой атаки «грубой силы» для различных вариантов знаний о ключе и количестве задействованных процессорных ядер.**

Сформируем текст с произвольным сообщением в формате «DEAR SIRS message THANKS» и загрузим его в шаблон.

Проведем 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. Зафиксируем затраты времени.

Выполним атаку повторно с средним и максимальным количеством процессорных ядер. Зафиксируем затраты времени.

Исходный текст:



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Известная часть ключа, байт | Время атаки грубой силы | | | |
| Количество ядер | | | |
| 1 | 2 | 3 | 4 |
| 14 | 1 секунда | 1 секунда | 1 секунда | 1 секунда |
| 12 | 29 минут | 19 минут | 15 минут | 14 минут |
| 10 | 1380 дней 22 часа | 829 дней 9 часов | 681 день | 668 дней 3 часа |

**3.6 Вывод.**

Из результатов выполнения данного пункта можно сделать вывод, что при увеличении количества задействованных ядер процессора, время атаки «грубой силы» уменьшается. Также использование открытого текста в качестве оценочной функции также уменьшает время атаки грубой силы по сравнению с использованием в качестве оценочной функции энтропии.

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

**4.1 Задание**

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

2. Подготовьтесь к атаке теоретически:

a. Изучите комментарии к шаблону

b. Изучите публикацию https://habrahabr.ru/post/247527/

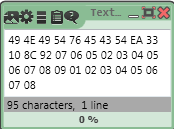
3. Внедрите во второй блок исходного текста коды символов своего имени.

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

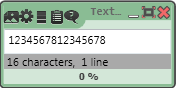
5. Убедитесь, что атака удалась.

**4.2 Исходные данные для экспериментов**

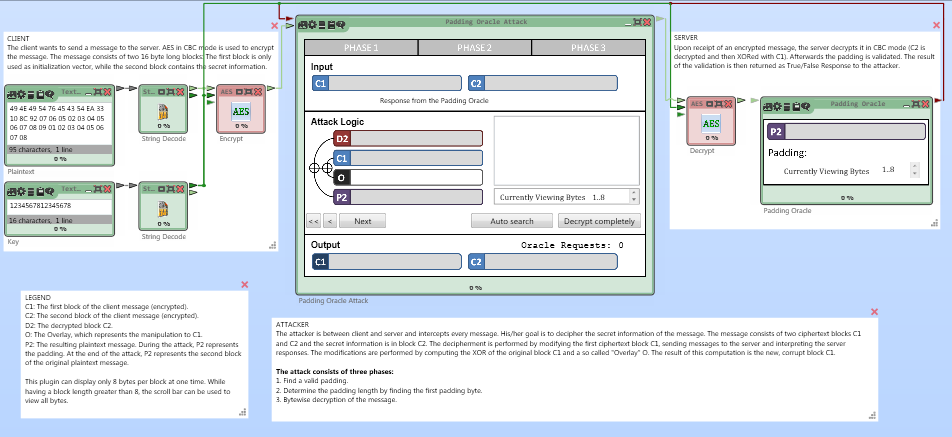
a. Исходный текст



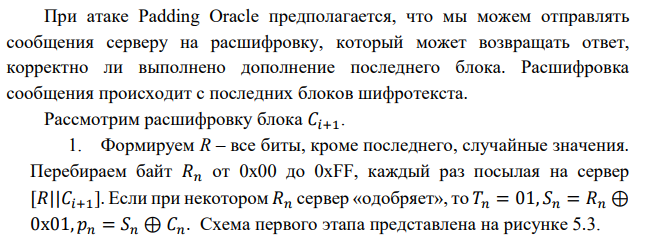
b. Секретный ключ

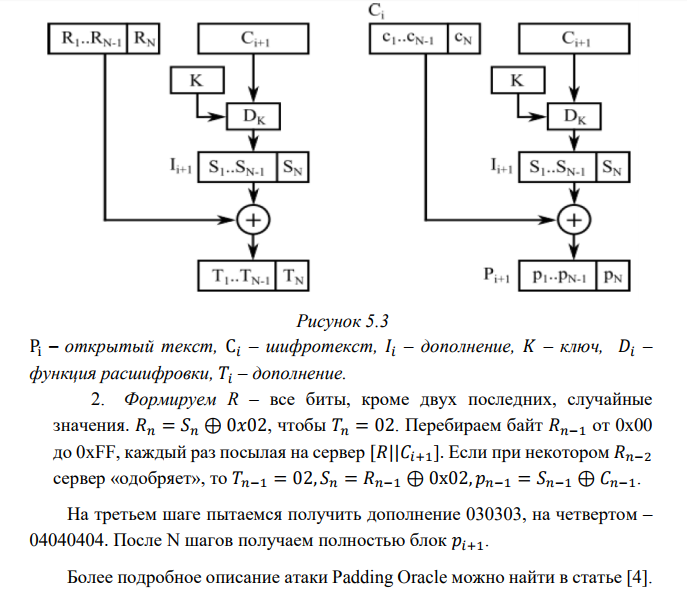


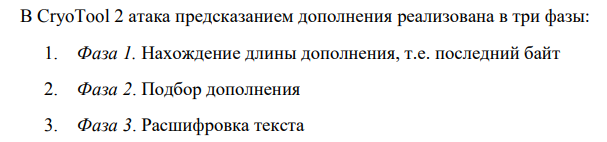
**4.3 Шаблон атаки «Padding Oracle Attack» из CrypTool 2**

****

**4.4 Описание атаки «Padding Oracle Attack».**

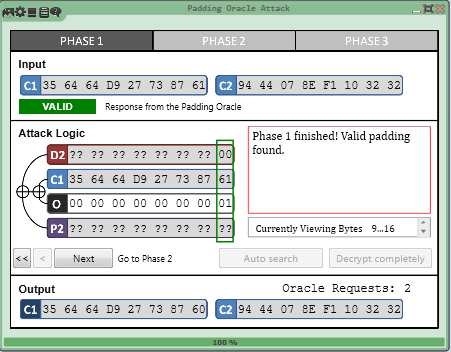
****

****

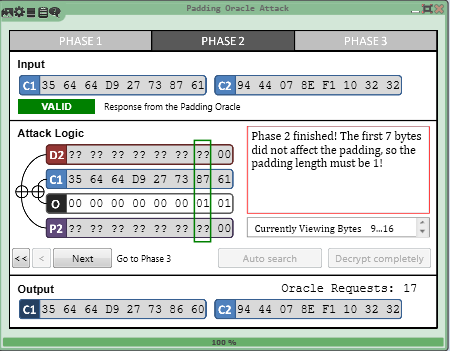
****

**4.5 Результаты 3-х фазы атак в виде итоговых скриншотов ПО.**

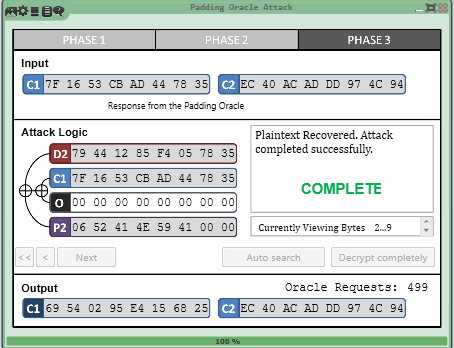
Результат фазы 1:



Результат фазы 2:



Результат фазы 3:



**4.6 Вывод**

Результатом выполнения данного пункта стало изучение атаки на шифр AES в режиме CBC (Padding Oracle Attack). Об успешно выполненной атаке свидетельствовало получение блока с корректным текстом после выполнения всех фаз алгоритма.

**5 Вывод**

В ходе выполнения данной лабораторной работы была изучена схема работы алгоритма AES. После изучения алгоритма с помощью демонстрационного приложения из CrypTool 1 были произведены расчет преобразований для первого раунда и первого раундового ключа. При проверке результатов с помощью приложения-инспектора расчеты совпали.

Также было проведено исследование финалистов конкурса AES. Результаты показали, что наибольшую энтропию имеет шифр Serpent. Также шифр Serpent оказался самым криптоустойчивым из рассмотренных шифров. Наименее устойчивыми к атаке «грубой силы» оказались шифры AES и RC6.

При изучении атаки «грубой силы» на AES был сделан вывод, что при увеличении количества задействованных ядер процессора, время атаки «грубой силы» уменьшается. Также использование открытого текста в качестве оценочной функции также уменьшает время атаки грубой силы по сравнению с использованием в качестве оценочной функции энтропии.

Также была изучена атака на шифр AES в режиме CBC (Padding Oracle Attack). Об успешно выполненной атаке свидетельствовало получение блока с корректным текстом после выполнения всех фаз алгоритма.

Несмотря на наименьшую устойчивость к атаке «грубой силы» по сравнению с другими финалистами конкурса AES, шифр AES такими важными достоинствами, как допуск параллельного выполнения преобразований раунда, удобная структура реализации, эффективная аппаратная и программная реализация на различных платформах.