**3. Основные структурные элементы алгоритма AES.**

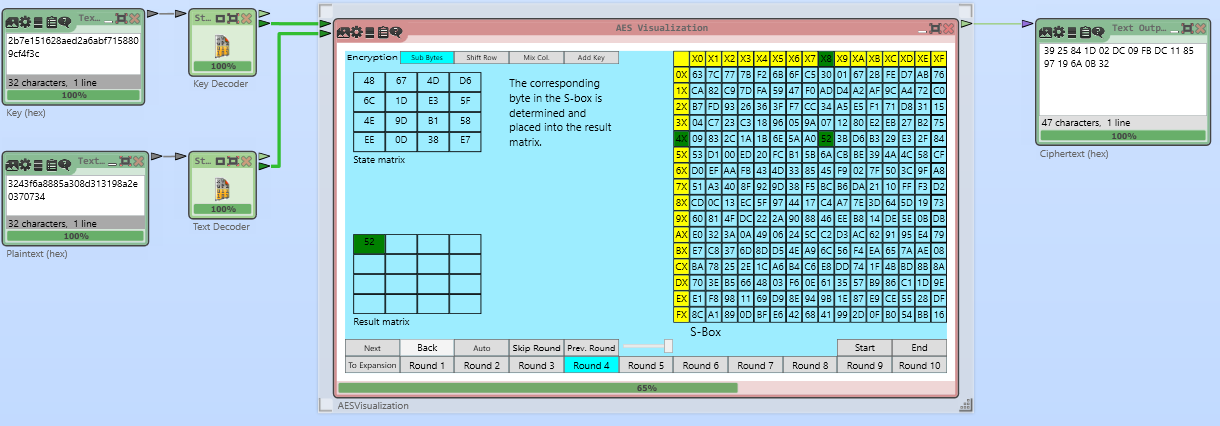
**Цель:** изучить основные принципы работы алгоритмы AES.

**Задачи практической работы**

1. Проанализировать эмуляцию алгоритма AES и примитивных атак на шифр, используя Cryptool 2. Выделить основные необходимые настройки шифра и требуемые ограничения на параметры.
2. Выполнение 1 цикла раундовой функции алгоритма AES вручную. Отразить промежуточные результаты шифрования после всех этапов алгоритма AES. Дать математическое обоснование для каждой операции. Также для подробного изучения шифра может быть использована программная реализация 1 раунда (или полной системы) AES в режиме отладки с выводом промежуточных значений шифрования.
3. Анализ принципов использования криптосистемы в современных приложениях на примере библиотеки openssl.

**Порядок выполнения работы.**

* + - 1. Для визуализации алгоритма AES предлагается использовать шаблон Cryptool 2 (Templates -> cryptography -> modern -> symmetric-> AES Visualization). Укажите в данном шаблоне свои входные данные и криптографический ключ.

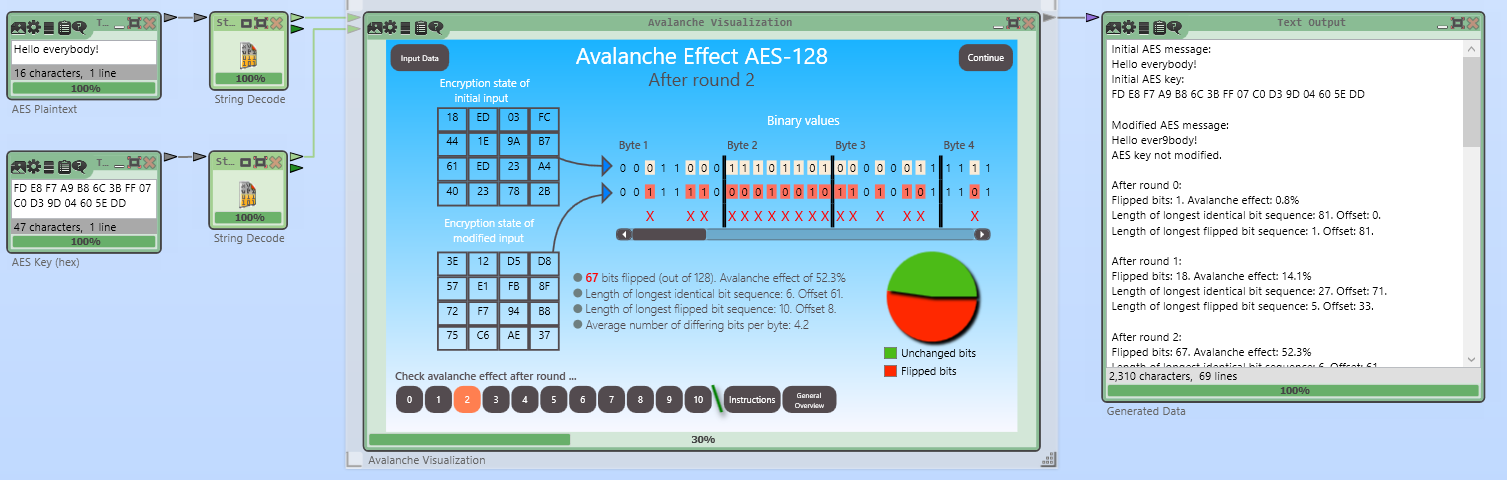


Проследите за каждым этапом выполнения процедуры шифрования криптоалгоритма AES. Рассмотрите подробно следующие операции:

* KeyExpansion;
* AddRoundKey;
* ShiftRows;
* MixColumn;
* SubBytes.

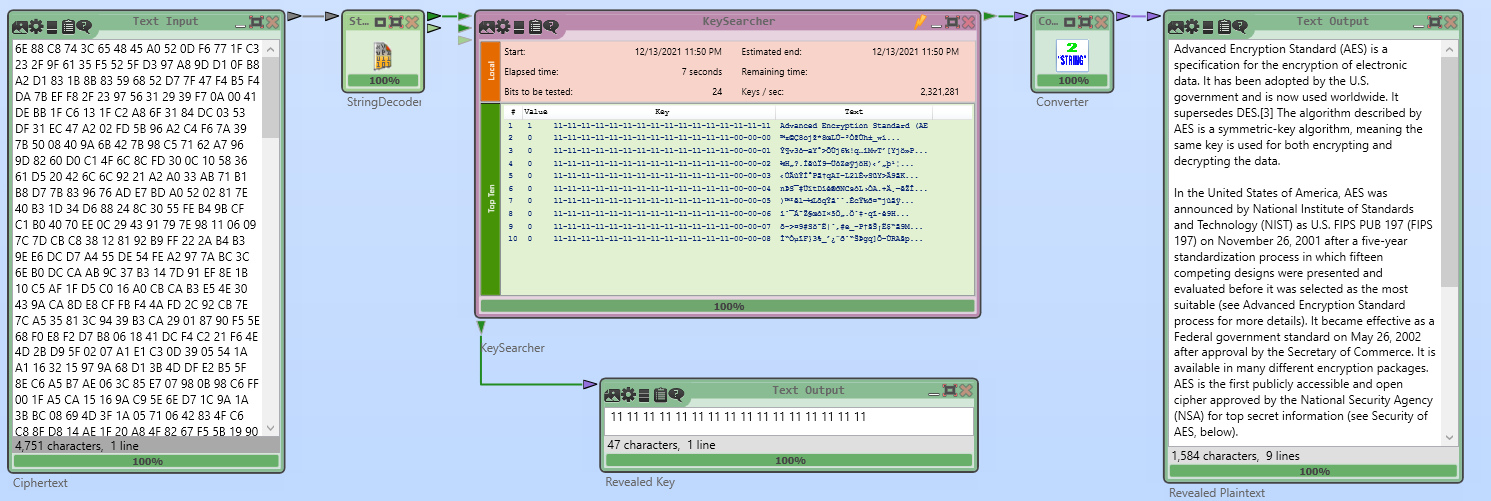
Обратите также внимание на то, как заполняется матрица состояний до начала работы шифра. Изучите последовательность выполнения операций при шифровании и дешифровании. Все ли раунды AES состоят из одинаковых операций? Проанализируйте каждое ли значение матрицы состояний меняется по результатам раунда AES.

* + - 1. Визуализация «лавинного эффекта» AES (templates -> cryptoanalysis -> modern -> avalanche (AES). Проследите за лавинным эффектом в процессе шифрования AES для своих значений открытого текста и ключа.

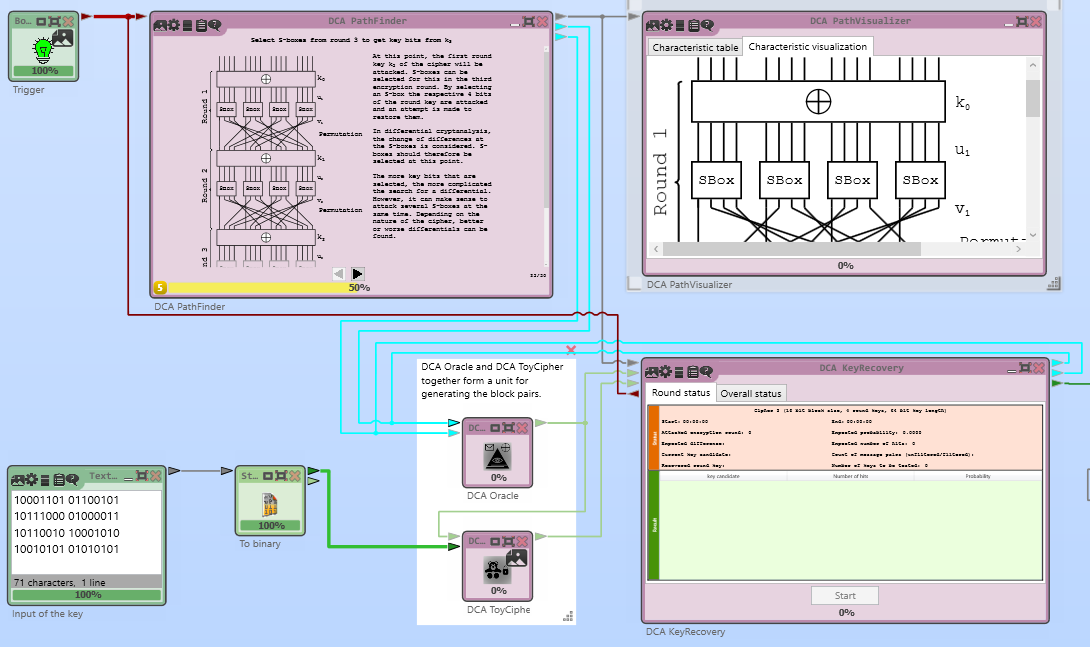


Отметьте процент искаженных битов в результате шифрования, скорость лавинного эффекта, как сгруппированы искаженные значения. Внесите искажения в несколько битов и проанализируйте характер лавинного эффекта.

1. Проведите атаку на основе известного открытого текста (шаблон templates->cryptanalysis->modern->AES known-plaintext analysis) на алгоритм AES для своих значений. Выделите этапы проведения атаки. Опишите ограничения, при которых рассматриваемая атака на криптоалгоритм становится возможной. Приведите примеры применения данной атаки в реальной жизни.



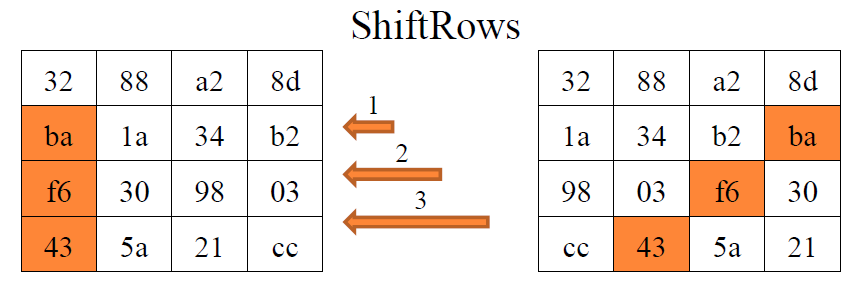
1. Изучите основные этапы проведения дифференциального анализа на блочные симметричные криптосистемы на примере шаблонов Differential Cryptanalysis Tutorial.



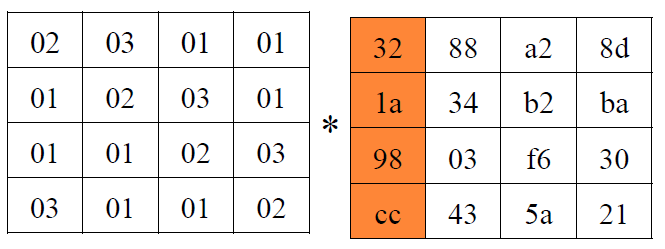
Опишите в отчете как происходит анализ таблиц нелинейной замены. Дайте краткое пояснение, что такое дифференциал и как он используется для подбора криптографического ключа.

1. Выполните 1 цикл раундовой функции алгоритма AES вручную. Для этого сгенерируйте случайное 128-битное значение входного сообщения и 128-битный раундовый ключ. Продемонстрируйте как выполняются следующие операции алгоритма AES:

* Процедура расширения криптографического ключа. Опишите сколько 32 битных слов генерируется для каждой длины криптографического ключа (128, 192, 256). Как слова, составляющие ключ, получаются из частей мастер ключа (операции, преобразования и пр.).
* Операция ShiftRows.

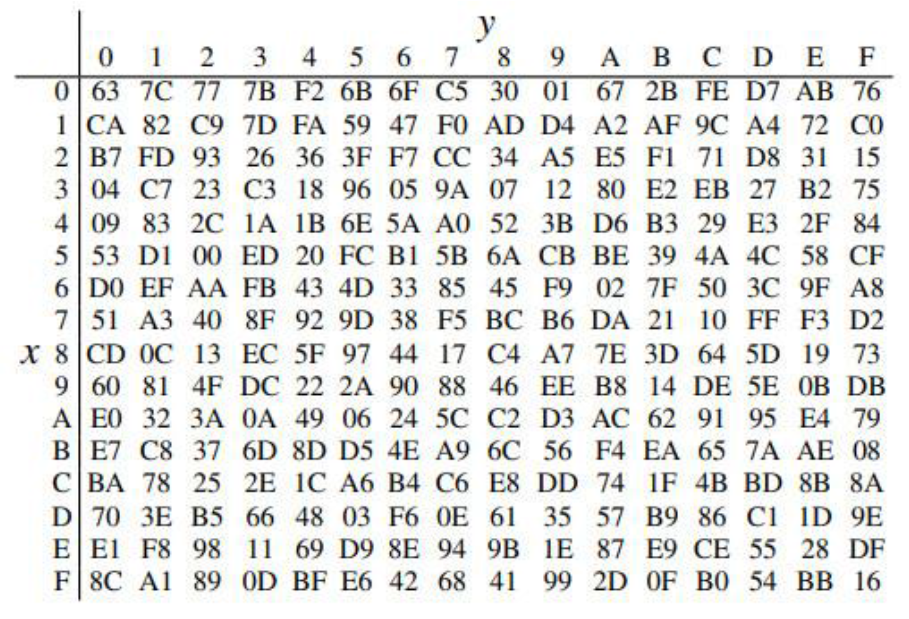


* побитовое сложение с ключом.
* операция MixColumn.



При рассмотрении операции MixColumn опишите как происходит преобразование шестнадцатеричных значений в элемент расширенного поля Галуа GF(2^8). В отчете дайте подробное описание процесса умножения элементов расширенного поля Галуа. Рассмотрите отдельно случай, когда при произведении элементов возможно переполнение, например, при произведении 02\*FF. Дайте описание операции InversionMixColumn, которое выполняет обратное действие для MixColumn. Какая матрица коэффициентов будет использоваться в качестве первого операнда при умножении матриц в InversionMixColumn? Можно ли операцию InversionMixColumn заменить несколькими операциями MixColumn?

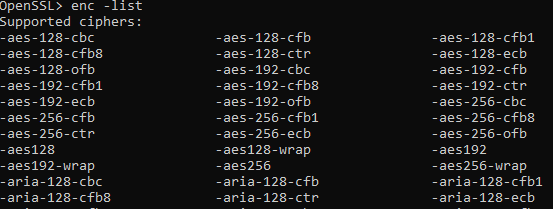
* Операция SubBytes



Опишите как работают представленные выше операции замены и перестановки. Результат выполнения операций для своих входных значений можно представить в виде:

* листов с отсканированным отчетом, на котором представлено рукописное выполнение необходимых этапов шифрования;
* листы отчета с этапами шифрования в электронном виде, который выполнен в любом удобном редакторе текстовых документов;
* листы с программным кодом или псевдокодом, которые выполняют вышепредставленные этапы алгоритма.

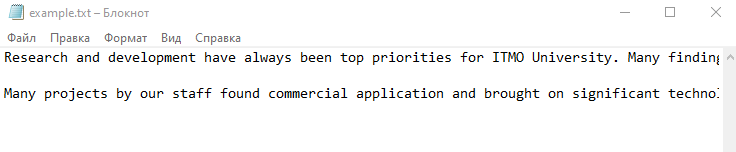
1. Выполните шифрование файла с помощью криптографической библиотеки OpenSSL. Для этого с помощью команды *openssl enc -list* выведите список доступных криптографических стандартов для шифрования.



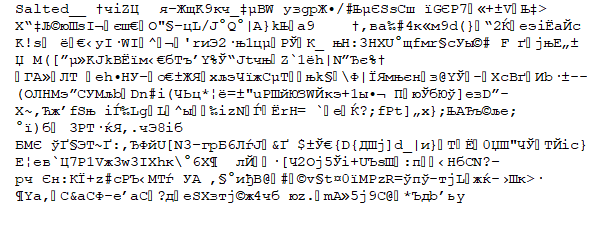
Выберите по крайней мере три подхода шифрования, включающих алгоритм AES, например, можно выбрать AES в нескольких режимах шифрования или с разными значениями криптографического ключа.

Задайте свое входное значение либо в виде файла, либо в виде сообщения в командной строке и зашифруйте их, используя 3 выбранных подхода шифрования с AES.





Файл example2.txt.enc, полученный после шифрования



Выполните дешифрование файла из предыдущего пункта. Проверьте получившийся открытый текст на ошибки. Проанализируйте следующие флаги и дополнительные параметры шифрования AES в OpenSSL: -salt, -a, -k, -iter. Как эти опции влияют на криптостойкость шифра?

**Альтернативный вариант** лабораторной предусматривает программную реализацию блочной симметричной криптосистемы, основанной на SP-сетях (не включая сеть Фейстеля). Реализуется шифр, вышедший не позже 1990 года, желательно выбирать шифры, которые включены в действующие стандарты шифрования отечественные или зарубежные. Для лабораторной работы достаточно реализовать один шифр, использующий SP-сеть. Основные процессы, которые необходимо реализовать в самом шифре:

* процесс шифрования;
* процесс дешифрования;
* процесс расширения ключей (получение подключей из мастер ключа).

Примеры шифров, на основе SP-сети, которые могут быть выбраны для реализации:

* AES
* ГОСТ 34.12 (часть 2, шифр с длиной блока 128 бит). Шифр Кузнечик
* IDEA
* Threefish
* SHARK

Нежелательна реализация упрощенных или легковесных шифров - шифры Present, miniAES и пр.

**Вопросы к защите.**

1. Классы эквивалентности
2. Группа, кольцо, поле
3. Теорема о существовании поля
4. Вычисления в простых и расширенных полях Галуа.
5. Использование расширенного алгоритма Евклида для нахождения мультипликативного обратного.
6. Малая теорема Ферма. Теорема Эйлера
7. Конкурс AES. Шифр Rijndael. Общие параметры криптосистемы.
8. Описание процедуры шифрования AES. Последовательность операций внутри раунда.
9. Краткое описание операций: shiftrows, subbytes, mixcolumn, addroundkey. Обратные операции: invshiftrows, invsubbytes, invmixcolumn, addroundkey, используемые при дешифровании
10. Процедура расширения ключа
11. ГОСТ 34.12. Кузнечик.