1. **Основные структурные элементы блочного симметричного алгоритма DES.**

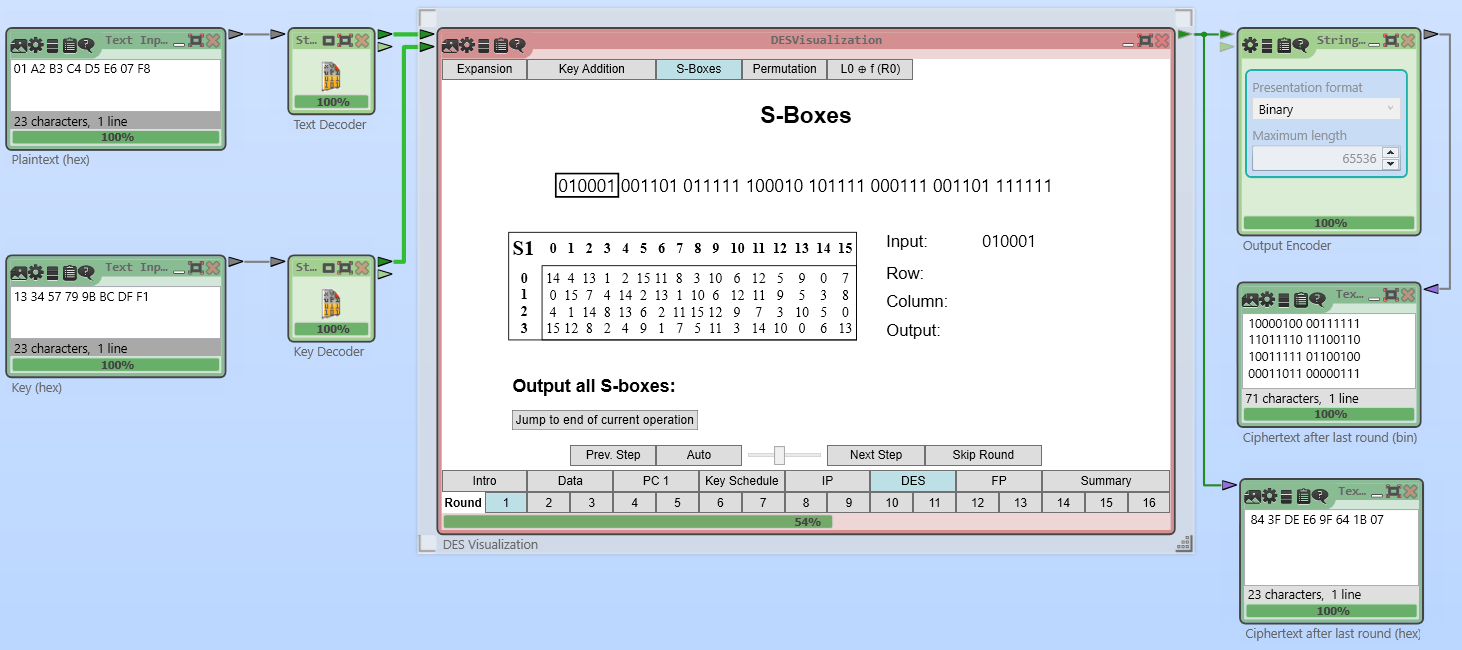
**Цель:** изучить основные принципы работы алгоритмы DES.

**Задачи практической работы**

1. Проанализировать эмуляцию алгоритма DES 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 DES вручную, то есть выполнение всех функций, входящих в раундовую функцию DES для фиксированного входного двоичного вектора с отображением промежуточных значений шифрования. Также для подробного изучения шифра может быть использована программная реализация 1 раунда (или полной системы) DES в режиме отладки с выводом промежуточных значений шифрования.
3. Анализ принципов использования криптосистемы в современных приложениях на примере библиотеки openssl.

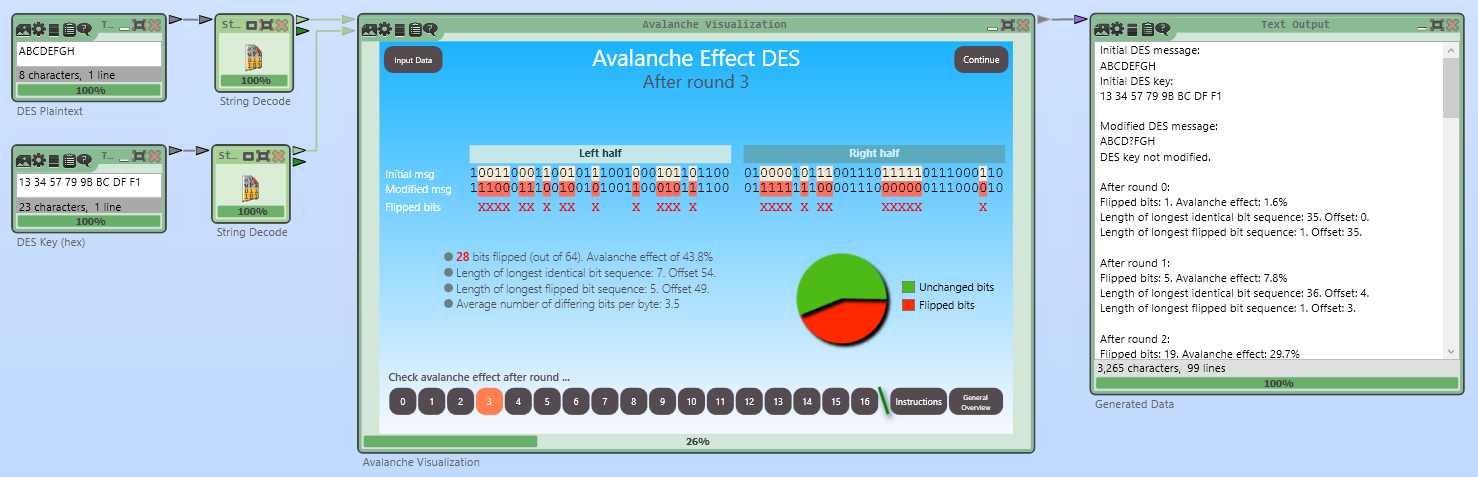
**Порядок выполнения работы.**

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



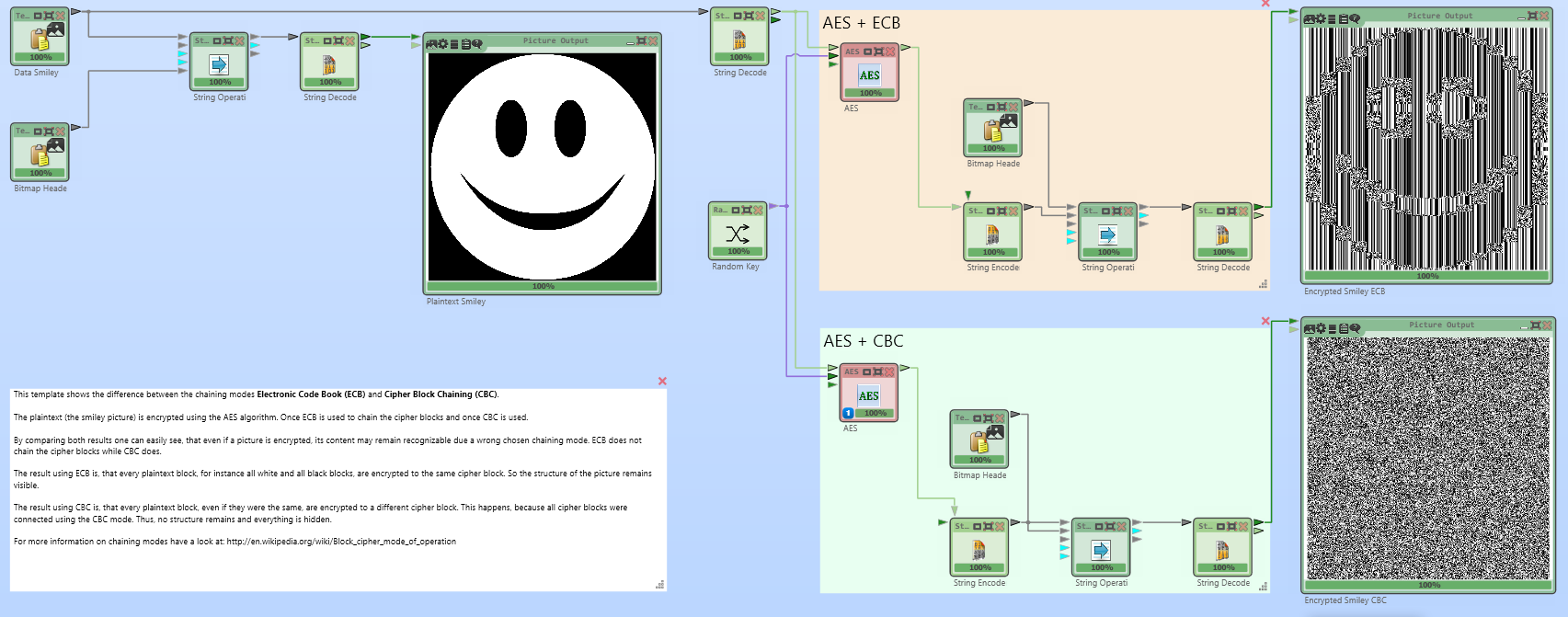
Проследите за поэтапным выполнением процедуры шифрования криптоалгоритма DES. Особое внимание уделите функции расширения ключа, структуре сети Фейстеля для алгоритма DES, этапам раундовой функции (перестановка с расширением E, сложение с ключом, нелинейная замена, прямая перестановка P). Отметьте, как изменяется длина подблоков после каждой итерации.

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



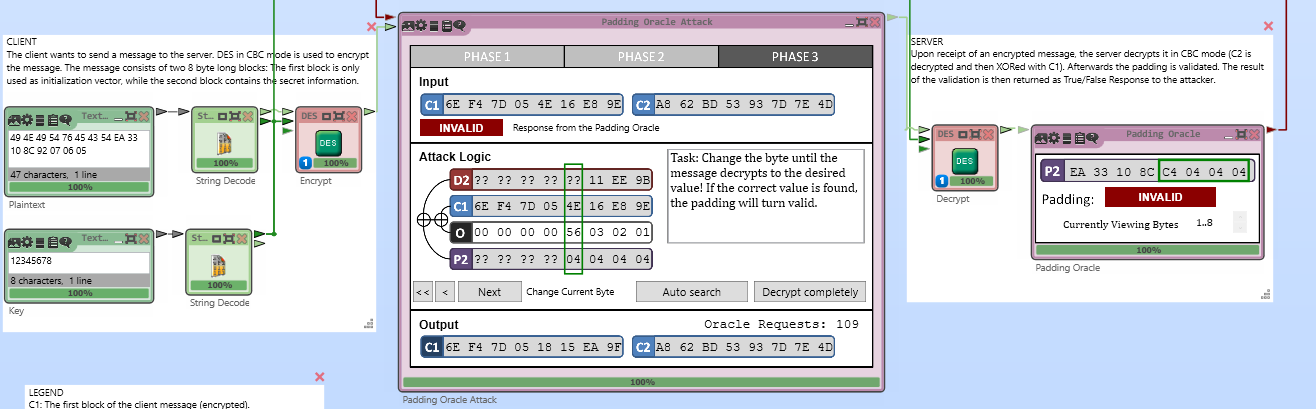
Отметьте процент искаженных битов в результате шифрования, скорость лавинного эффекта, характер группировки искаженных значений. Внесите искажения в несколько битов и проанализируйте характер лавинного эффекта. Внесите искажения в промежуточные значения шифрования на 10, 12, 14 раундах, проследите за тем, каких значений достигнет лавинный эффект.

1. Изучите принципы работы различных режимов шифрования блочных симметричных шифров, используя шаблон Cryptool 2 Templates -> cryptography -> modern ->Block Modes of Symmetric Ciphers



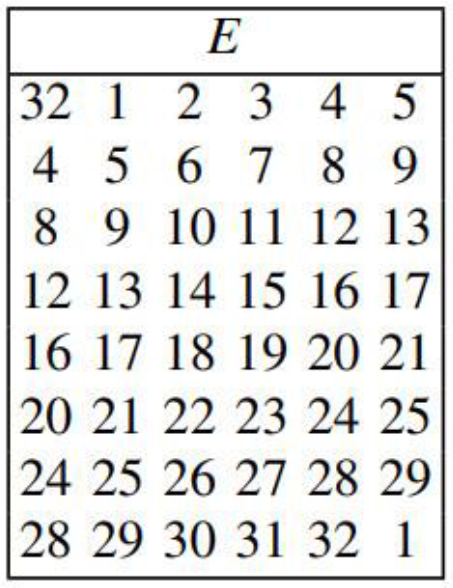
Отметьте в чем опасность использования режима шифрования ECB с точки зрения информационной безопасности. Изучите другие режимы шифрования и способы сцепления блоков (режимы CBC, CFB, OFB, RD, CTR, GCM).

1. Проведите padding oracle атаку на алгоритм DES для своих значений. Выделите этапы проведения атаки. Приведите примеры применения данной атаки в реальной жизни

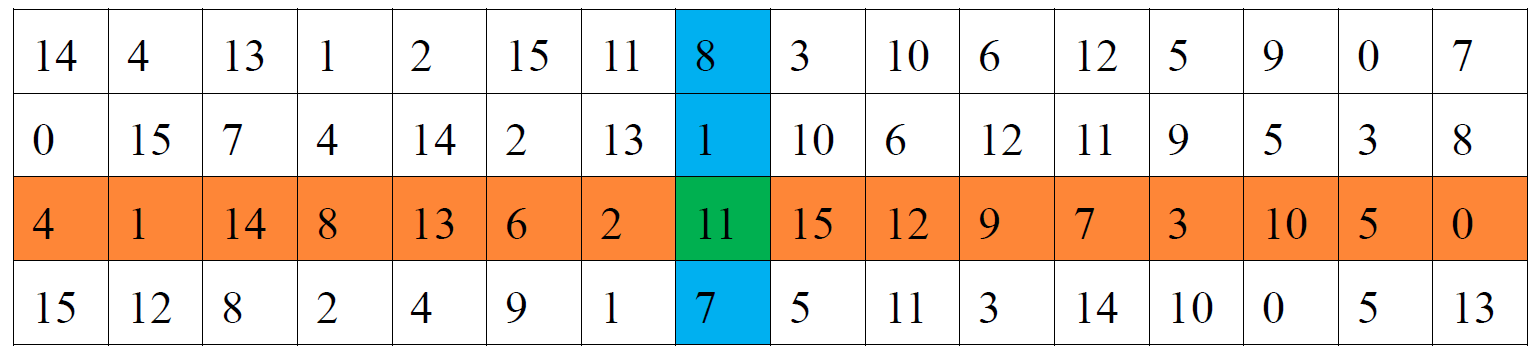


1. Выполните 1 цикл раундовой функции алгоритма DES вручную. Сгенерируйте случайное 32-битное значение входного сообщения и 48-битный раундовый ключ. Продемонстрируйте как выполняются следующие операции алгоритма DES:

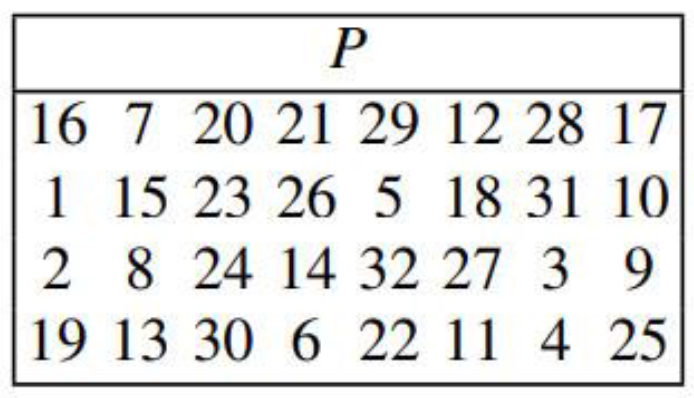
* перестановка с расширением E;



* побитовое сложение с ключом;
* операция подстановки (S-box);



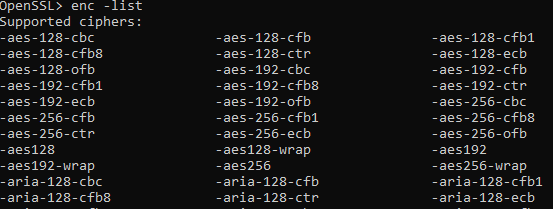
* прямая перестановка P.



Опишите как использовать представленные выше таблицы 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.

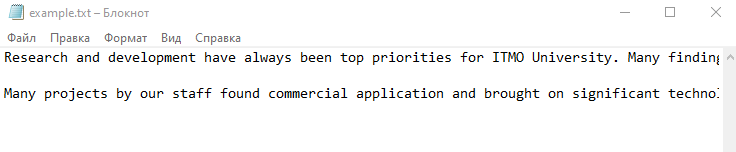
1. Выполните шифрование файла с помощью криптографической библиотеки OpenSSL. Для этого с помощью команды *openssl enc -list* выведите список доступных криптографических стандартов для шифрования



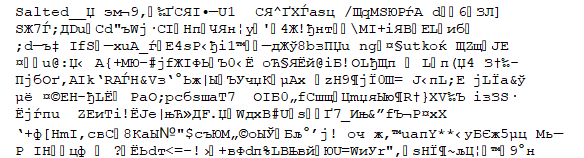
Выберите по крайней мере три подхода шифрования, включающих алгоритм DES, например, можно выбрать DES в нескольких режимах шифрования или несколько модификаций 3DES.

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





Файл example.txt.enc, полученный после шифрования



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

**Альтернативный вариант** лабораторной предусматривает программную реализацию блочной симметричной криптосистемы, основанной на сети Фейстеля (не путаем понятие SP-сети и сети Фейстеля. Сеть Фейстеля - частный случай SP-сети). Для лабораторной работы достаточно реализовать полностью один шифр, использующий сеть Фейстеля. Основные процессы, которые необходимо реализовать

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

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

* DES
* ГОСТ 34.12 (часть 1, шифр с длиной блока 64 бита). Шифр “Магма” (старое название ГОСТ 28147)
* RC6
* Blowfish
* FEAL
* KASUMI (из стандарта GSM)

Еще один вариант - реализация потокового шифра, например, подойдет любой из шифров-участников конкурса eStream (https://ru.wikipedia.org/wiki/ESTREAM).

**Вопросы к защите**

1. Симметричные блочные и потоковые шифры.
2. Синхронные и асинхронные потоковые шифры.
3. Сферы применения потоковых шифров.
4. Одноразовый шифр-блокнот
5. Регистры сдвига с линейной обратной связью
6. GSM Протокол A5/2
7. Необходимость вектора инициализации в потоковых шифрах.
8. Шифр Trivium.
9. Шифр Rabbit
10. Свойства конфузии и диффузии в блочных шифрах.
11. Сеть Фейстеля
12. Алгоритм DES. Процедуры шифрования/дешифрования. Расширение ключа.
13. Техника отбеливания ключа
14. 3DES
15. ГОСТ 28147 или блочный шифр с длиной блока 64 бита из ГОСТ 34.12.
16. Режимы шифрования ECB, CBC, CFB, OFB, CTR, GCM. Устойчивость к атакам вставки и удаления блоков. Лавинный эффект. Возможность параллельной обработки блоков.
17. Код аутентификации сообщения
18. Схемы хэширования на основе блочных симметричных криптосистем.