Лабораторная работа №3

Объединение блочных шифров

Цель работы: ознакомится с принципами объединения блочных шифров и алгоритмом 3DES. Разработать консольное приложение, использующее для шифрования и расшифрования алгоритм 3DES.

Задание:

1. Разработать консольное приложение, реализующее шифрование/расшифрование файла по алгоритму 3DES EDE (Encrypt-Decrypt-Encrypt) с использованием следующих режимов сцепления блоков:
    - 3DES ECB;
    - 3DES Inner CBC;
    - 3DES Outer CBC;
    - 3DES with pad;
    - native 3DES (если есть в вашей криптографической библиотеке - https://pycryptodome.readthedocs.io/en/latest/src/cipher/des3.html).

    Для шифрования использовать три разных ключа. Ключи записывать в файл в бинарном виде без разделителей.

    Инициализирующий вектор размером 8 байт также записывать в бинарном виде в отдельный файл.
2. Сравнить производительность алгоритма с каждым режимом сцепления блоков, произведя замеры времени шифрования и расшифрования файлов размером 1МБ, 5МБ, 10МБ, 50МБ, 100МБ. Визуализировать результаты в виде графиков или столбчатых диаграмм.
3. Сделать вывод по полученным данным, соотнести его с информацией о криптостойкости каждого из решений, выбрать оптимальный метод сцепления блоков.

Требования к консольному приложению

Консольное приложение должно иметь три режима:

- генерация ключа;
- шифрование файла;
- расшифрование файла.

Консольное приложение должно принимать на вход следующие аргументы:

- режим работы;
- режим шифрования;
- путь к файлу для шифрования/расшифрования (если требуется);
- путь к файлу для сохранения зашифрованного/расшифрованного файла (если требуется);
- путь к файлу с инициализирующим вектором (если требуется);
- путь к файлу с ключом.

Приветствуется использование аргументов командной строки для передачи вышеописанных параметров. Наличие интерактивного режима не обязательно - при его отсутствии или при запуске с неверными аргументами приложение должно показывать инструкцию по использованию.

Ключ для 3DES состоит из трех ключей DES. Для хранения ключа использовать бинарный формат, записывать все три ключа подряд без разделителей.

О реализации приложения

Выбор языка не ограничен.

Для реализации шифрования 3DES использовать методы для DES.

В случае, если в выбранном модуле/библиотеке имеется реализация 3DES с использованием каких-либо из режимов сцепления - реализовать все режимы сцепления 3DES самостоятельно. В эксперименте сравнить производительность полученных реализаций с представленными в модуле/библиотеке и сделать выводы.

Об объединении блочных шифров и эксперименте

Текст лекции об объединении блочных шифров

Прошу в этот раз подойти к эксперименту внимательней. Приведите в отчете все графики, требуемые в задании. Ко всем полученным результатам применяем радикальное сомнение, проверяем результаты на соответствие здравому смыслу (чтобы 1МБ не шифровался дольше, чем 100МБ и так далее).

Контрольные вопросы

1. Для чего применяется объединение блочных шифров?
2. Виды объединения блочных шифров существуют.
3. В чем заключается принцип многократного шифрования?
4. Виды многократного шифрования.
5. В чем заключается принцип каскадного шифрования?
6. Пример безопасного каскадного шифрования.
7. Примеры объединения блочных шифров, используемых на практике.
8. Режимы сцепления блоков в 3DES.