Лабораторная работа №1

Работа с CNG

Цель работы: ознакомится с криптографическим API операционных систем семейства Windows. Разработать консольное приложение, использующее CNG для генерации ключа и шифрования/дешифрования файлов. Исследовать лавинный эффект при разных режимах сцепления блоков.

Задание:

1. Разработать консольное приложение, позволяющее генерировать ключи шифрования и шифровать/дешифровать файлы симметричным шифром AES с использованием криптографического API CNG.
2. Исследовать лавинный эффект при разных режимах сцепления блоков (ECB, CBC, CFB). В ходе исследования нужно
    a. произвести эксперимент по изменению каждого отдельного бита в открытом тексте;
    b. построить график зависимости количества измененных в шифротексте битов от позиции измененного бита в открытом тексте.

Требования к консольному приложению:

Язык разработки - C.

В качестве аргументов приложение должно принимать режим работы (генерация ключа, шифрование, дешифрование) и набор аргументов, необходимый для выполняемой операции:

- для генерации ключа:
    - [out] путь к файлу ключа
- для шифрования:
    - [in] путь к файлу ключа
    - [in] путь к файлу для шифрования
    - [in] режим сцепления блоков
    - [out] путь к инициализирующему вектору
    - [out] путь к зашифрованному файлу
- для дешифрования:
    - [in] путь к файлу ключа
    - [in] путь к инициализирующему вектору
    - [in] путь к зашифрованному файлу
    - [in] режим сцепления блоков
    - [out] путь к расшифрованному файлу

Кроме того, необходимо общепринятым образом обработать несоответствие переданных программе аргументов ожидаемым - сообщить о несоответствии и показать инструкцию.

Порядок знакомства с документацией

Начать все-таки следует с основного раздела документации - общей информации о CNG.

Далее нужно так же пробежаться взглядом по фичам (там в конце есть информация по режимам сцепления блоков) и криптографическим примитивам.

Чтобы уложить общий флоу работы с CNG на примере - идем в раздел Using CNG и смотрим примеры программ. Там же вы и найдете обещанный пример шифрования.

Читая код обращайте внимание на порядок вызова функций. Даже если кажется, что в общем-то понятно, что функция делает - берем ее название и идем в справочную информацию по CNG, где находим описание всех констант, документацию к методам и так далее.

Лавинный эффект

Лавинный эффект — важное криптографическое свойство для шифрования, которое означает, что изменение значения малого количества битов во входном тексте или в ключе ведет к «лавинному» изменению значений выходных битов шифротекста. Другими словами, это зависимость всех выходных битов от каждого входного бита.
Для исследования лавинного эффекта можно сделать отдельное приложение, которое будет использовать общий код с вашим консольным приложением или же вызывать ваше приложение, например с использованием функции *system*.

В отчете должны присутствовать графики зависимости количества изменившихся бит от позиции инвертированного бита в изменяемом объекте. Таким образом, для полноты эксперимента необходимо произвести инвертирование каждого бита изменяемого объекта.

Кроме того, отчет должен содержать вывод о характере лавинного эффекта и о его зависимости от изменяемого объекта и позиции инвертируемого бита.

Порядок сдачи

С вопросами, дополнениями, предложениями обращаться в онлайн туда, где проводятся лекции (discord).

Сдача будет происходить в порядке получения мною ваших работ.

О сдаче лабораторных из лекции

При защите буду обращать внимание на вызываемые в коде методы и их аргументы. От вас будет требоваться ознакомиться с документацией и знать:

- что делает метод
- какие аргументы принимает (сигнатура метода)
- что значит эта константа, которую вы передаете в качестве аргумента
- какие еще могут быть константы (не все возможные, а просто для понимания)

Для тех кто не пишет код самостоятельно сдавать будет труднее, потому что они недостаточно времени потратили на ознакомление с документаций.

Из чего должен состоять отчет:

- цель работы
- ход работы по пунктам:
    - каждый этап выполнения задания
    - какие методы использовались
    - с чем столкнулись в ходе реализации
- код
- результаты работы программы

- вывод (исходя из целей работы, возникших сложностей, используемых инструментов и деталей реализации)

Материалы:

- https://msdn.microsoft.com/en-us/library/windows/desktop/aa376210(v=vs.85).aspx - документация
- http://www.intuit.ru/studies/courses/600/456/lecture/10202 - лекция на интуите
- http://xakep.ru/42665/ - статья с хакера
- https://www.codeopenssl speed -evp aes-128-cbcproject.com/Articles/18713/Simple-Way-to-Crypt-a-File-with-CNG - сборка проекта с CNG