МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №2

“Изучение шифра DES”

Студент гр. 8382 Мирончик П.Д.

Преподаватель Племянников А.К.

Санкт-Петербург

2021

ВЫВОДЫ

1. Исследование DES

Был исследован шифр DES. Рассмотрена схема шифрования (рис. 1.1), разобраны ее этапы: исходная перестановка, раунды, конечная перестановка. Отдельно рассмотрен процесс генерации ключей: исходная перестановка, исключающая каждый 8-й бит, деление на субблоки, сдвиг субблоков при генерации каждого следующего раундового ключа и объединение субблоков, из которых в результате сжимающей перестановки получаются раундовые ключи. Описана также схема реализации раундовой функции: расширяющая перестановка, сложение с раундовым ключем, замена получившихся 8 субблоков по таблице замен, завершающая перестановка.

Была разработана программа, осуществляющая шифрование и расшифрование блока текста по описанному выше алгоритму DES (приложение А), проведено ее тестирование на примере исходного текста *mironchi* и ключа *030208d*. В результате шифрования был получен фрагмент с кодами символов `31 189 74 9 3 254 201 8`, который затем был успешно расшифрован с применением той же программы. Процесс дешифрования был описан теоретически, но сами этапы преобразований расписаны не были, поскольку они полностью дублировали этапы преобразований для шифрования, за исключением реализации раундов (также потому, что получить полную информацию можно запуском программы). Процесс зашифрования описан максимально подробно (п. 1.3).

2. Режимы ECB и CBC шифра DES

Рассмотрены основные параметры режимов ECB и CBC.

ECB – шифрование в режиме DES по блокам, при этом следующий зашифрованный блок не зависит от предыдущего. ECB позволяет проводить шифрование блоков быстрее за счет параллельной обработки, а также благодаря независимости блоков обеспечивается устойчивость к ошибкам

(неправильное зашифрование одного блока не приведет к порче остальных блоков). Тем не менее, при зашифровании в режиме ECB одинаковые блоки будут одинаковыми и в зашифрованном виде, а также появляется уязвимость в виде возможности замены любого блока без повреждения других.

CBC – шифрование, в котором для каждого следующего блока выполняется сложение с зашифрованным предыдущим блоком. В отличие от ECB, ошибка в одном блоке распространяется на все следующие, однако при дешифровке происходит самовосстановление; одинаковые блоки будут в результате преобразованы в разные. Последний блок можно использовать в качестве контроля целостности сообщения. Тем не менее, CBC не позволяет провозить параллельное шифрование различных блоков.

На рис. 2.4 и рис. 2.5 наглядно показаны различия в шифровании одинаковых блоков в режимах ECB и CBC. CBC дает гораздо больше шума в сообщении, однако зашифрованное этим режимом сообщение практически невозможно сжать.

Для ECB и CBC было проведено исследование зависимости времени атаки грубой силы от известной длины ключа. Выяснено, что при известных четырех байтах подбор занимает около получаса, для двух известных байт – уже около года. CBC показал при этом несколько лучшие результаты с точки зрения устойчивости.

3. 3-DES

3-DES – шифр DES, примененный трижды. Существуют различные модификации шифра 3DES, отличающиеся длиной ключа и средней операцией – шифрование или дешифрование.

Очевидно, что шифр 3-DES более устойчив к атаке грубой силы в сравнении с DES, т.к. имеет большую длину ключа – время подбора ключа атакой грубой силы показано в табл. 3.1 и табл. 3.2. Режим CBC опять показал несколько лучшие результаты в сравнении с режимом ECB.

Выяснено, что CrypTool 1 использует EDE2 реализацию шифра (см. п. 3.5).

4. DESX, DESL, DESXL

В заключение были рассмотрены шифры DESX, DESL и DESXL. Выяснено, что DESX представляет собой модифицированный вариант DES с 184-битным ключем, формула шифрования которого выглядит как

$$\mathrm{DESX(M)} = \mathrm{K_2} \oplus \mathrm{DES_K(M} \oplus \mathrm{K_1)}$$

DESL – облегченный вариант DES без начальной и конечной перестановок, а DESXL – комбинация DESX и DESL шифров.

Установлено, что все три шифра обладают одинаковой энтропией. Также для шифров проведен анализ атаки грубой силы, который показал, что DESX и DESXL примерно одинаково устойчивы к атакам грубой силы, а шифр DESL требует примерно вдвое меньше времени для подбора ключа, чем шифр DES. Вероятно, это связано с тем, что в шифровании DESL меньше операций, т.к. удаление операций начальной и конечной перестановок не влияют на криптостойкость шифра.