**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра информационной безопасности**

отчет

**по лабораторной работе №4**

**по дисциплине «Криптография и защита информации»**

Тема: Изучение шифра DES

|  |  |  |
| --- | --- | --- |
| Студент гр. 8383 |  | Киреев К.А. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

**Выводы.**

* Изучен демонстрационный пример шифра DES, представленный в CrypTool. Выполнен ручной расчет субблоков и раундовых ключей шифра для первых двух раундов. Ключ и исходный текст были заданы.
* Изучены два режима шифра DES – ECB и CBC.
  1. При использовании шифра DES в режиме ECB блоки кодируются независимо с использованием одного и того же ключа шифрования, благодаря чему сохраняется однородность зашифрованных данных там, где она присутствовала в исходном изображении. Однородные данные хорошо подаются сжатию с одной стороны, и проще в расшифровке с другой.
  2. При использовании режима CBC изображение превращается в шум. Однако такие неоднородные данные почти не поддаются сжатию.
* Проведены попытки взлома ключа методом “грубой силы” в режимах ECB и CBC.
  1. Были выявлены закономерности:
     1. Если известная длина ключа составляет до 4 байт включительно, то скорость атаки на шифротекст в режиме CBC возрастает в полтора-два раза.
     2. С уменьшением известной длины ключа скорость атаки в обоих случаях существенно понижается.
* Рассмотрен шифр 3-DES в четырех его версиях.
  1. Экспериментальным путем была выявлена используемая в программе CrypTool реализация 3-DES – DES-EDE2.
* Проведены попытки взлома ключа методом “грубой силы” шифра 3-DES.
  1. В ходе анализа атаки “грубой силой” шифра 3-DES в режимах ECB и CBC было выявлено, что шифр является довольно безопасным, так как, зная 10 байт из возможных 16, время дешифровки займет больше двух лет.
* Изучены шифры DESX, DESL, DESXL.
  1. Выявлено, что шифрование DESX, DESL, DESXL имеет примерно одинаковую эффективность. Эти значения примерно в два раза больше, чем у исходного текста, что означает внешнюю псевдослучайность шифротекста.
* Исследовано время расшифровки текста при полном отсутствии информации о секретном ключе.
  1. Шифры DESX и DESXL показали гораздо лучший результат, чем шифр DESL.