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

ОТЧЕТ

по лабораторной работе №5
по дисциплине «Криптография и защита информации»
Тема: Изучение шифра AES

Студент гр. 8383 _____ Киреев К.А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург
2021

Выводы.

- Изучен демонстрационный пример шифра AES. Шифр AES использует структуру «Квадрат». На вход получает блок текста размером 128 бит и ключ (128, 192, 256 бит) в шестнадцатеричной системе счисления. Каждый раунд, за исключением последнего, состоит из 4 слоев: подстановки, перемешивание строк, перемешивание столбцов, XOR с раундовым ключом.
- Произведен расчет преобразований для первого раунда и первого раундового ключа. При проверке результатов с помощью приложения-инспектора расчеты совпали.
- Проведен анализ финалистов конкурса AES. По результатам видно, что значения энтропии для каждого из 5 шифров примерно одинаковы и заметно выше, чем у исходного текста, что говорит о надежности шифра. Наибольшее значение (6.13) получено при использовании Twofish. Все шифры показали почти одинаковое время расшифровки при известной части ключа от 10 байт, что говорит о хорошей криптостойкости шифров. По соотношению энтропии и времени атаки самый эффективный шифр – Twofish.
- Проведена атака «грубой силой» на шифр. Временные затраты на дешифовку с использованием максимального количества ядер (8) составили 1157 дней, что означает высокую криптостойкость шифра. Выявлено, что с увеличением количества ядер уменьшается время на дешифровку. Проведение атаки со знанием части открытого текста и использованием его в качестве оценочной функции ускоряет процесс дешифровки примерно в 2 раза. Так, при знании 12 байт ключа и использовании 3 ядер время уменьшается с 52 минут до 25.
- Проведена атака на шифротекст методом Padding Oracle Attack. По изображениям видно, что атака прошла успешно и второй блок исходного текста был правильно дешифрован. Более того, произошло 495 обращений к серверу из возможных 4080, что в разы меньше, чем атака «грубой силой».