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

ОТЧЕТ

по лабораторной работе №5

по дисциплине «Криптография и защита информации»

Тема: Изучение шифра AES

Студент гр. 8383 _____ Ларин А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург

2021

Выводы.

1. Был исследован шифр AES. Был изучен алгоритм его работы, воспроизведён вручную, результат сравнен с машинной обработкой. Результаты совпали.
2. Была изучены другие финалисты конкурса AES: Rijndael, MARS, RC6, Serpent, Twofish.

   Был выбран текст, после чего зашифрован всеми шифрами. По итогу произведено сравнение параметров энтропии и сложность атаки грубой силой при различной известной части улюча. Значение энтропии получились очень похожими.

   Результаты атаки были немого различны, так Serpent оказался примерно в три раза более криптостойким, однако разница во всех случаях оказалась менее порядка, т. е. AES(Rijndael) существенно не уступает конкурентам
3. Была произведена атака грубой силой на AES при оценочной функции энтропии и известного словосочетания, а так же при отхном количестве ядер и известных байт ключа

   В результата количество ядер дало пропорциональный прирост к скорости. оценочная функция по словосочетанию показала немного лучший результат. Однако никакое из этих преимуществ не является решающим, т. к. при малой известной длине ключа они не взламываемы за разумное время вне зависимости от количества ядер.
4. Была изучена Атака предсказанием дополнения на шифр AES в режиме CBC (Padding Oracle Attack), основанная на знании правил формирования паддинга, а так же аозможности отправлять серверу сообщения для расшифровки

   Изучен теоретический принцип её работы, а так же реализация в Cryptool 2, с разделением на три фазы.

   В первой фазе найден байт первого блока, при котором получается верное дополнение

Во второй фазе последовательным изменением байт слева направо найдена длина доплнения. После чего в третьей фазе, инкрементируя дополнение и поиск валидного по ответам сервера, побайтово найден весь промежуточный блок, который при XOR с первым блоком шифротекста (принцип CBC) дал открытый текст. Открытый текст совпадал с исходным, в т.ч. содержал буквы имени.