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

ОТЧЕТ

по лабораторной работе №5

“Изучение шифра AES”

Студент гр. 8382 Мирончик П.Д.

Преподаватель Племянников А.К.

Санкт-Петербург

2021

ВЫВОДЫ

В ходе выполнения работы был разобран алгоритм работы шифра AES для 128-битного ключа. Описана реализация алгоритма, включая операции внутри раунда и процедуру генерации раундовых ключей.

В качестве проверки теоретического материала было выполнено ручное шифрование одного блока текста для одного раунда. Результат зашифрования был успешно проверен с использованием функций визуализации CrypTool 1.

Проведен сравнительный анализ шифров AES, MARS, RC6, Serpent и Twofish, основанный на проведении энтропийной атаки и атаке грубой силы. Определено, что MARS, RC6, Serpent и Twofish не имеют решающего преимущества перед AES с использованием рассмотренных атак.

Далее на шифр AES были проведены текстовая и энтропийная атаки с использованием различного (1, 3 и 6) количества ядер процессора и известных байт ключа. На используемых исходных данных результаты атак показали сравнимую эффективность.

Также была рассмотрена Padding Oracle Attack на шифр AES. Изучен алгоритм проведения атаки, и проведена пробная атака средствами CrypTool 2. В результате атаки текст оказался успешно дешифрован и получено исходное значение.