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

ОТЧЕТ

по лабораторной работе №6

“Изучение хэш-функций”

Студент гр. 8382 Мирончик П.Д.

Преподаватель Племянников А.К.

Санкт-Петербург

2021

4. Исследование лавинного эффекта md5, sha-1, sha-256, sha-512

При исследовании лавинного эффекта были исследованы хеш-функции MD5, SHA-1, SHA-256, SHA-512 и получены результаты по количеству измененных бит хеша при изменении части исходного текста: добавлении, удалении или изменении одного символа. Определено, что, с учетом длины хеша, функции показывают примерно одинаковый результат.

5. Хэш-функция SHA-3

В ходе исследования хеш-функции SHA3 был рассмотрен ее алгоритм. Визуализирован с использованием CrypTool 2 процесс раундовых преобразований и показан результат этих преобразований в виде сгенерированного хеша. Проведена оценка лавинного эффекта и определено, что процент измененных бит в сравнении с хешем исходного текста составляет примерно 53%.

6. Контроль целостности по коду HMAC

В ходе изучения контроля целостности по коду HMAC было проведено практическое исследование возможности определить подлинность текста – его соответствие отправленному передающей стороной. На основе ключа и согласованных с принимающей стороной параметров HMAC был сгенерирован хеш для исходного текста. Принимающая сторона получила хеш, исходный и измененный тексты, и, сгенерировав хеши для каждого из полученных текстов, определила подлинный, не подвергавшийся изменениям.

4. Атака дополнительной коллизии на хеш-функцию

Была исследована атака дополнительной коллизии на хеш функцию. Рассмотрен ее принцип действия на примере парадокса “дня рождения”, а также проведена атака с использованием средств CrypTool 1 для 16 совпадающих бит. Проведена оценка временных затрат на проведение атаки для 24-128 совпадающих бит, результаты которой представлены в табл. 3.