Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет информационных технологий и управления
Кафедра интеллектуальных информационных технологий
Дисциплина «Средства и методы защиты информации в интеллектуальных системах»

ОТЧЁТ
к лабораторной работе №7
на тему
«УСТАНОВКА, ИСПОЛЬЗОВАНИЕ И АНАЛИЗ СПЕЦИАЛИЗИРОВАННЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОГО ПАКЕТА OPENSSL»

БГУИР 6-05-0611-03 130

Выполнил студент группы 321701
СЕМЕНЯКО Владимир Дмитриевич

_____
(дата, подпись студента)

Проверил
САЛЬНИКОВ Даниил Андреевич

_____
(дата, подпись преподавателя)

Минск 2025

1 ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

а) Установить OpenSSL и ознакомиться с возможностями библиотеки (команда «?»).

б) Выполнить тестирование скорости выполнения различных алгоритмов шифрования.

в) Создать криптографические ключи. Выбрать несколько произвольных файлов и выполнить:

– шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;

– шифрование (зашифрование и расшифрование) посредством различных асимметричных алгоритмов;

– хэширование различных файлов различными алгоритмами (обязательно md5 и sha1).

– создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.

2 ВЫПОЛНЕНИЕ РАБОТЫ

Algorithm	1024 B	8192 B	16384 B
AES-128-CBC	964311.38	974735.67	974760.33
DES-EDE3	20483.08	20512.99	20482.74

Таблица 2.1 – Скорость симметричного шифрования для ключевых размеров блоков (kB/s)

RSA Key (bits)	Sign/s	Verify/s	Encrypt/s	Decrypt/s
512	33127.2	387330.1	327630.4	27183.7
1024	6282.5	125622.7	133178.8	6400.4
2048	1090.4	43978.8	34555.5	884.2
3072	377.9	20548.6	20114.9	376.3
4096	173.1	11928.2	11738.5	172.9
7680	21.1	3465.9	3410.1	21.0
15360	3.7	814.7	876.5	3.9

Таблица 2.2 – Производительность RSA для различных размеров ключей (операции в секунду)

Algorithm	1024 B	8192 B	16384 B
SHA1	1204357.22	1444650.95	1460236.50

Таблица 2.3 – Скорость хэширования SHA1 для ключевых размеров блоков (kB/s)

Результаты хэширования файла с текстом Hello OpenSSL Test 1

– MD5(file1.txt) = 53f41d08791fae7bde168b1b9f511378
– SHA1(file1.txt) = 92a7ef306456bee6ed7831ea9c912c929468568d
– SHA2-256(file1.txt) = 13ec453d3fbd42e6e465317bead1f7518823aa4...

Ниже приведено текстовое описание самоподписанного сертификата X509

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            42:b8:26:38:3b:7f:1b:c8:f2:18:2e:77:2a:7f:9f:ee:cf:f4:ab:e7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BY, ST=Minsk, L=Minsk, O=Company123, OU=IT, CN=Vladimir, emailAddress=semenyakovladimir@gmail.com
        Validity
            Not Before: Oct 19 20:23:17 2025 GMT
            Not After : Oct 19 20:23:17 2026 GMT
        Subject: C=BY, ST=Minsk, L=Minsk, O=Company123, OU=IT, CN=Vladimir, emailAddress=semenyakovladimir@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b4:1b:ba:a8:48:5c:0d:bb:20:69:21:1c:7f:d5:
                    0f:ba:fa:11:42:70:82:8d:92:d5:ed:44:82:52:24:
                    d0:bf:a7:a6:ac:39:e5:b1:55:49:e4:e0:b6:4b:dd:
                    27:31:1c:0f:48:1e:46:c4:67:27:0f:7d:e0:8b:bd:
                    59:94:dd:e6:cd:ef:6c:2b:be:0f:49:13:29:b5:27:
                    d3:26:ba:68:c2:b4:79:8f:4b:44:61:f5:39:76:23:
                    84:e7:81:32:40:ad:9e:36:2d:21:d0:2f:f9:e1:3e:
                    13:ff:93:03:6a:60:ff:a3:ad:db:ac:71:68:b3:84:
                    51:0a:a4:9e:eb:d8:36:dd:55:c1:9b:5b:71:41:6a:
                    9a:3e:1d:d4:59:7a:18:01:b5:46:ff:49:02:58:15:
                    fb:20:2f:8c:aa:27:cb:b6:dc:71:db:70:bc:07:50:
                    04:2a:bd:d9:c0:1c:96:ca:9d:ac:47:82:d8:23:7a:
                    74:33:16:58:51:95:a9:92:e1:88:fc:bb:3d:36:da:
                    93:03:15:ba:ca:0c:68:4e:98:12:66:ea:6b:4b:4e:
                    39:26:9a:74:58:9f:db:d2:b4:d7:44:f3:73:54:7b:
                    3b:8a:ec:97:f5:cf:5b:12:c9:53:bf:a9:53:cb:02:
```

Рисунок 1 – Содержание самоподписанного сертфиката

ВЫВОД

В ходе лабораторной работы были изучены принципы работы библиотеки OpenSSL и основные механизмы криптографической защиты данных. В процессе выполнения задания были проведены тесты производительности различных алгоритмов шифрования, создано несколько типов криптографиче-

ских ключей, выполнено симметричное и асимметричное шифрование и расшифрование файлов, а также вычислены хэш-значения с использованием алгоритмов MD5, SHA1 и SHA256. Дополнительно был создан и проанализирован самоподписанный сертификат X.509, изучена его структура и назначение компонентов. Полученные результаты позволили оценить различия в скорости и особенностях работы симметричных и асимметричных алгоритмов, а также закрепить практические навыки использования инструментов OpenSSL для обеспечения безопасности данных.