Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №7 по теме: «УСТАНОВКА, ИСПОЛЬЗОВАНИЕ И АНАЛИЗ СПЕЦИАЛИЗИРОВАННЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОГО ПАКЕТА OPENSSL»

Студент гр. 121702

Колтович Д.С.

Проверил:

Сальников Д.А.

Минск 2023

Тема

Установка, использование и анализ специализированных средств криптографического пакета OpenSSL.

Задание

1) Установить OpenSSL на виртуальную машину (или рабочую версию ОС Windows 7/8/10 пользователя) и ознакомиться с возможностями библиотеки (команда «?»).

2) Выполнить тестирование скорости выполнения различных алгоритмов шифрования.

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

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

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

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

4) Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.

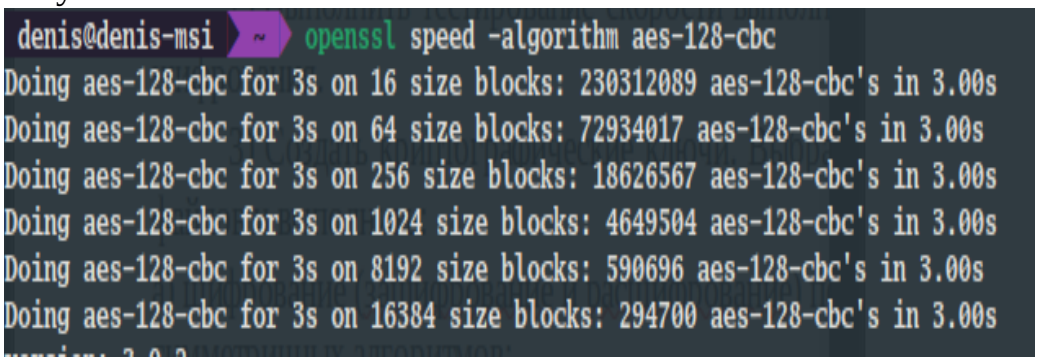
Выполнение задания

Задание 1 на Ubuntu

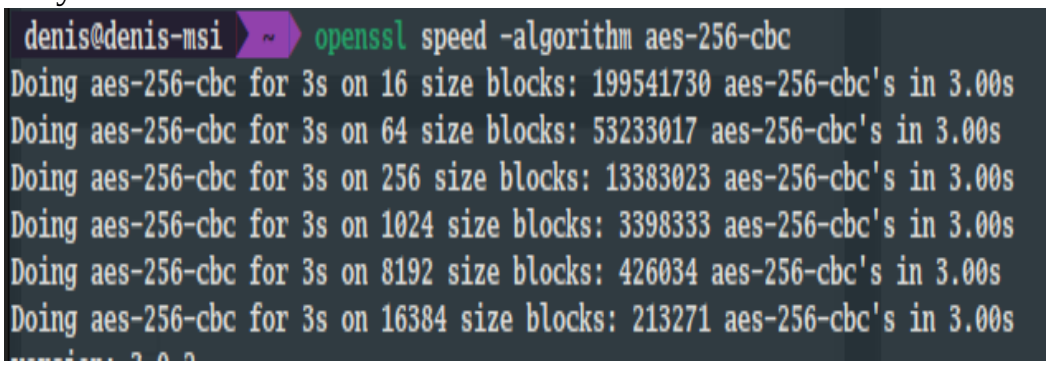
```
zsh: no matches found: ?
✘ denis@denis-msi ~ openssl help
help:

Standard commands
asn1parse         ca                ciphers           cmp
cms               crl               crl2pkcs7         dgst
dhparam           dsa               dsaparam          ec
ecparam           enc               engine            errstr
fipsinstall       gendsa            genpkey           genrsa
help              info              kdf               list
mac               nseq              ocsp              passwd
pkcs12            pkcs7             pkcs8             pkey
pkeyparam         pkeyutl           prime             rand
rehash            req               rsa               rsautl
s_client          s_server          s_time            sess_id
smime             speed             spkac             srp
storeutl          ts                verify            version
x509

Message Digest commands (see the `dgst' command for more details)
blake2b512        blake2s256        md4               md5
rmd160            sha1              sha224            sha256
sha3-224          sha3-256          sha3-384          sha3-512
sha384            sha512            sha512-224        sha512-256
shake128          shake256          sm3

Cipher commands (see the `enc' command for more details)
aes-128-cbc       aes-128-ecb       aes-192-cbc       aes-192-ecb
aes-256-cbc       aes-256-ecb       aria-128-cbc      aria-128-cfb
aria-128-cfb1     aria-128-cfb8     aria-128-ctr      aria-128-ecb
aria-128-ofb      aria-192-cbc      aria-192-cfb      aria-192-cfb1
aria-192-cfb8     aria-192-ctr      aria-192-ecb      aria-192-ofb
aria-256-cbc      aria-256-cfb      aria-256-cfb1     aria-256-cfb8
aria-256-ctr      aria-256-ecb      aria-256-ofb      base64
bf                bf-cbc            bf-cfb            bf-ecb
bf-ofb            camellia-128-cbc  camellia-128-ecb  camellia-192-cbc
camellia-192-ecb  camellia-256-cbc  camellia-256-ecb  cast
cast-cbc          cast5-cbc         cast5-cfb         cast5-ecb
cast5-ofb         des               des-cbc           des-cfb
des-ecb           des-ede           des-ede-cbc       des-ede-cfb
des-ede-ofb       des-ede3          des-ede3-cbc      des-ede3-cfb
des-ede3-ofb      des-ofb           des3              desx
rc2               rc2-40-cbc        rc2-64-cbc        rc2-cbc
rc2-cfb           rc2-ecb           rc2-ofb           rc4
rc4-40            seed              seed-cbc          seed-cfb
seed-ecb          seed-ofb          sm4-cbc           sm4-cfb
sm4-ctr           sm4-ecb           sm4-ofb
```

Задание 2

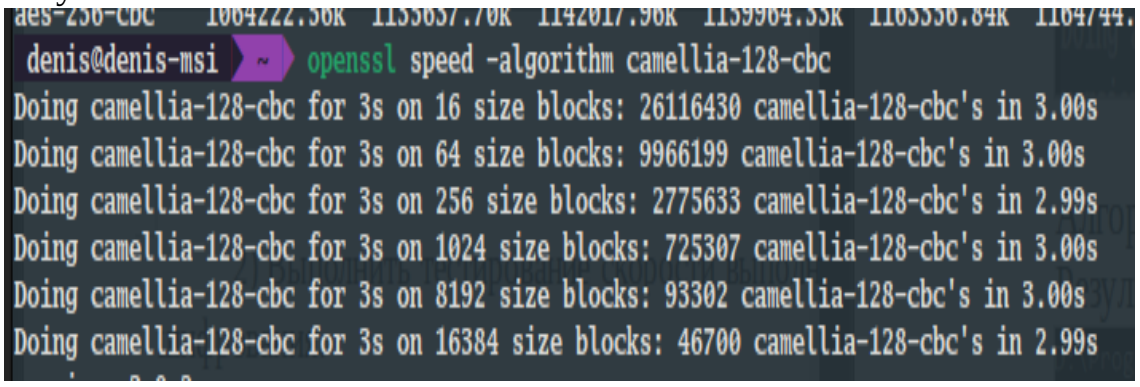
Алгоритм: aes-128-cbc
Результаты



Алгоритм: aes-256-cbc
Результаты



Алгоритм: camellia-128-cbc
Результаты



Алгоритм: camellia-256-cbc
Результаты

```
camellia-128-cbc   159287.65k   212012.25k   237646.17k   247571.46k   254776.66k   255
 denis@denis-msi  ~  openssl speed -algorithm camellia-256-cbc
Doing camellia-256-cbc for 3s on 16 size blocks: 21961254 camellia-256-cbc's in 2.99s
Doing camellia-256-cbc for 3s on 64 size blocks: 7723028 camellia-256-cbc's in 3.00s
Doing camellia-256-cbc for 3s on 256 size blocks: 2144155 camellia-256-cbc's in 3.00s
Doing camellia-256-cbc for 3s on 1024 size blocks: 555588 camellia-256-cbc's in 3.00s
Doing camellia-256-cbc for 3s on 8192 size blocks: 69262 camellia-256-cbc's in 3.00s
Doing camellia-256-cbc for 3s on 16384 size blocks: 32178 camellia-256-cbc's in 2.98s
```

Результат выдаётся в виде количества килобайтов, обработанных за ~3с.
Большее значение означает лучший результат

Задание 3

А)Алгоритм aes-128-cbc
Ключ: password

```
original text
 denis@denis-msi  ~/bsuir/Crypto/lab7  5sem ±  openssl enc -aes-128-cbc -in original.txt
-out encrypted.txt
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
```

```
 denis@denis-msi  ~/bsuir/Crypto/lab7  5sem ±  cat encrypted.txt
Salted__
```

```
 denis@denis-msi  ~/bsuir/Crypto/lab7  5sem ±  openssl enc -d -aes-128-cbc -out original.
txt -in encrypted.txt
enter AES-128-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
 denis@denis-msi  ~/bsuir/Crypto/lab7  5sem ±  cat original.txt
original text
```

Алгоритм camellia-256-cbc
Ключ: password

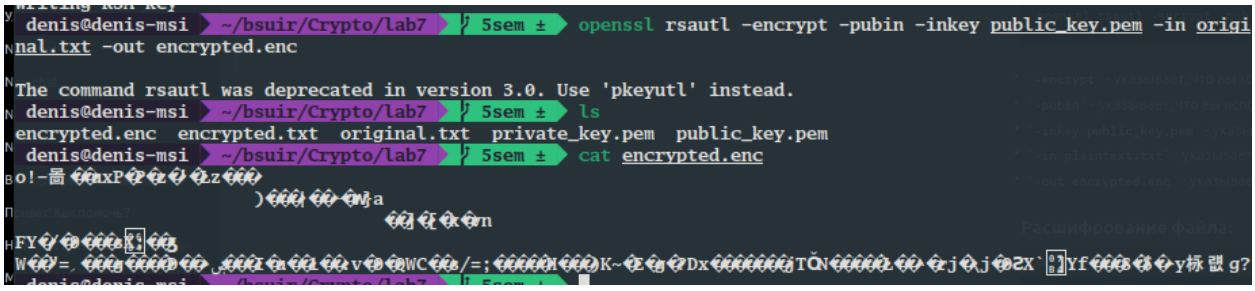
```
 denis@denis-msi  ~/bsuir/Crypto/lab7  5sem ±  openssl enc -camellia-256-cbc -in original
.txt -out encrypted.txt
enter CAMELLIA-256-CBC encryption password:
Verifying - enter CAMELLIA-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```
Salted__^K9<94><91>iaÕ^?~jP<8d>¿^L^[:)¯EÏÊÁ;8
```

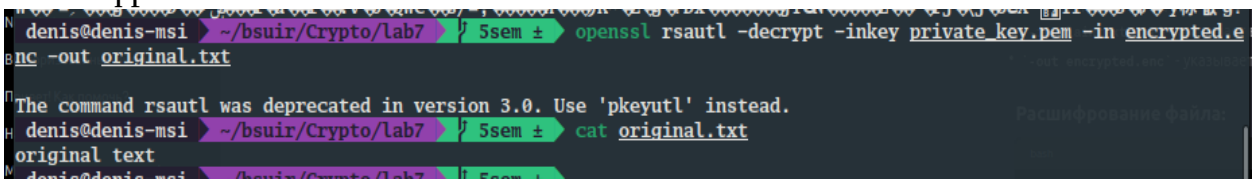
```
 denis@denis-msi  ~/bsuir/Crypto/lab7  5sem ±  openssl enc -d -camellia-256-cbc -out orig
inal.txt -in encrypted.txt
enter CAMELLIA-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
 denis@denis-msi  ~/bsuir/Crypto/lab7  5sem ±  cat original.txt
original text
```

Б) Алгоритм RSA
Генерация ключей:

Зашифрованный текст:

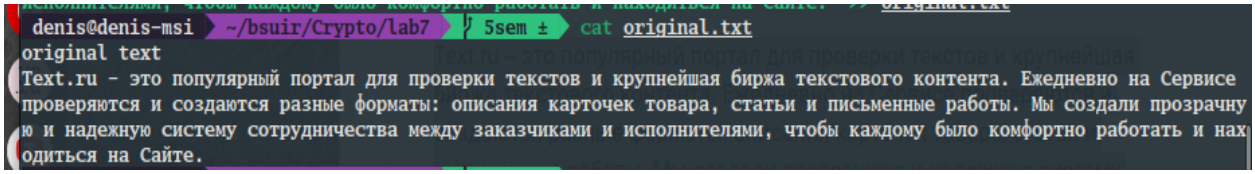


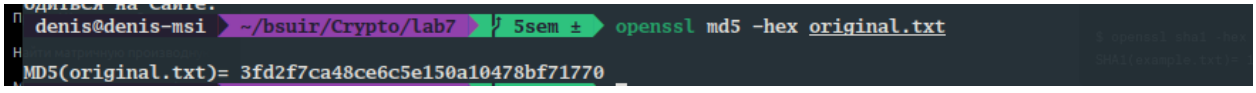
Расшифрованный текст:

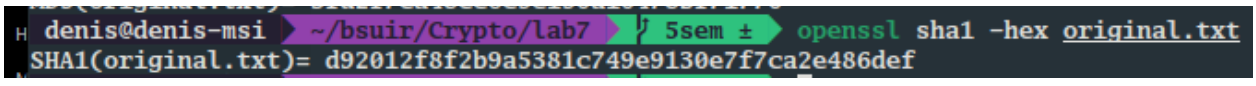


B)Алгоритм хеширования MD5

Оригинальный текст:







```
denis@denis-msi ~/bsuir/Crypto/lab7 5sem ± openssl sha256 -hex original.txt
SHA256(original.txt)= 690e6f9871c53b4a985db57e6185a58821aebf307a345929e2240e9d59c37138
```

Задание 4

Создание сертификата:

```
denis@denis-msi ~/bsuir/Crypto/lab7 5sem ± openssl req -new -x509 -key private_key.pem -out self_signed_certificate.pem

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Minsk
Locality Name (eg, city) []:city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BSUIR
Organizational Unit Name (eg, section) []:AI
Common Name (e.g. server FQDN or YOUR name) []:Denis
Email Address []:koltov
```

Состав сертификата:

```
denis@denis-msi ~/bsuir/Crypto/lab7 5sem ± openssl x509 -in self_signed_certificate.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:1e:e0:6e:91:61:f6:7b:8f:f9:4a:bc:9d:ab:d3:2c:49:4b:c9:04
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = RU, ST = Minsk, L = city, O = BSUIR, OU = AI, CN = Denis, emailAddress = koltov
        Validity
            Not Before: Nov 23 17:48:03 2023 GMT
            Not After : Dec 23 17:48:03 2023 GMT
        Subject: C = RU, ST = Minsk, L = city, O = BSUIR, OU = AI, CN = Denis, emailAddress = koltov
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a6:c9:5c:20:62:4c:60:7b:dd:b1:19:2d:3d:59:
                    8c:ec:42:2b:fb:3c:60:45:69:df:f0:5a:c7:6d:e7:
                    e1:88:0a:12:cc:0d:5f:c3:9b:5a:52:cd:84:5a:9a:
                    c4:a7:f7:52:85:a4:5c:c7:d6:67:05:41:eb:2f:6c:
                    d0:2b:ab:38:27:b2:7c:cd:d1:15:f3:75:e6:7c:34:
                    88:a5:50:f7:79:ab:f5:ff:ca:81:83:01:c9:8e:08:
                    d1:f4:18:7c:38:e5:8d:54:e7:37:53:26:63:19:c2:
                    51:c0:87:2d:78:20:be:a1:3b:fd:be:15:f1:15:bc:
                    f3:b6:61:11:38:47:a9:28:38:31:49:fd:5f:ab:71:
                    a5:e3:4c:2d:34:21:cc:57:29:ab:49:7b:92:cf:23:
                    d4:c4:34:98:ef:6c:77:91:5c:36:08:6d:84:96:7a:
                    ce:cd:f5:e9:c6:66:5d:2a:f9:31:10:b5:38:53:90:
                    51:7c:2d:a5:09:9a:cf:65:3d:a5:0f:3f:13:bd:f8:
                    a8:70:f8:1a:de:19:76:3a:ab:a0:70:49:9e:92:85:
                    30:43:43:d7:c3:74:45:16:b0:26:81:6c:51:29:a9:
                    5a:f7:8b:78:9a:87:24:86:28:ae:41:61:20:37:c9:
                    86:a1:82:d9:12:77:f6:c1:ba:92:f8:a5:98:99:7d:
                    4c:41
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                BF:3B:58:26:AE:68:81:B1:60:AC:EA:F9:6D:4F:6F:7F:E7:62:B2:31
            X509v3 Authority Key Identifier:
                BF:3B:58:26:AE:68:81:B1:60:AC:EA:F9:6D:4F:6F:7F:E7:62:B2:31
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        04:ec:74:d6:ad:ad:c3:ce:21:cd:f2:cf:c7:df:17:2a:44:10:
        4d:c0:7c:da:d7:4d:a6:de:3e:72:f8:d7:8d:8e:83:35:70:63:
        4d:51:28:0c:2a:b1:99:08:3f:35:77:fb:3c:04:23:30:ee:9e:
        19:83:71:e4:ef:19:84:64:32:cd:17:1a:a8:f9:3a:ca:0e:8f:
        38:93:79:b8:c9:c8:13:61:06:21:b8:28:15:d5:59:3e:92:6a:
        c3:a5:6d:5e:19:99:34:31:5c:92:ec:d3:d4:6c:d4:81:bc:30:
        91:16:04:d7:41:aa:a0:f5:d7:f4:11:7f:0b:fa:92:f2:62:34:
        8a:bf:f9:d5:81:d8:94:68:9e:21:8c:bd:06:f9:f1:c3:d8:e2:
        3b:09:f6:d5:44:1e:2e:43:e1:9e:aa:b9:49:f6:a7:43:74:c0:
        e2:33:75:64:9b:e2:9d:98:0d:8c:26:76:5f:cc:0a:9a:17:43:
        05:ed:79:4d:58:15:ab:00:62:4d:c9:b1:17:e9:74:f7:5c:bd:
        59:8f:ee:a1:9e:6b:3b:e0:00:eb:00:3d:a2:80:72:a1:03:84:
        cb:d9:8a:1d:d9:db:ee:3c:33:68:03:37:93:b1:76:99:eb:6f:
        06:65:e1:47:0d:ac:a2:47:90:90:a7:ae:a7:0e:c4:82:d0:ac:
        95:20:35:fc
```

Сертификат X509 содержит в себе следующую информацию

1. Имя владельца сертификата
2. Издатель сертификата
3. Информация об открытом ключе
4. Серийный номер сертификата
5. Период действия сертификата
6. Дополнительные детали
7. Идентификатор издателя
8. Идентификатор субъекта

Вывод

В ходе лабораторной работы были получены основы работы с библиотекой OpenSSL. Данная библиотека обладает обширными возможностями в области криптографии: хеширование, шифрование. Были рассмотрены различные алгоритмы шифрования и хеширование. Также был создан сертификат стандарта X.509.