Министерство образования Республики Беларусь

Учреждение Образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра ИИТ

Лабораторная работа № 4

«УСТАНОВКА, ИСПОЛЬЗОВАНИЕ И АНАЛИЗ СПЕЦИАЛИЗИРОВАННЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОГО ПАКЕТА OPENSSL»

Выполнил: Ахроров М. Д.

Студент группы: 921731

Принял: Захаров В. В.

Минск 2021

**1. Цель работы**

Изучить и научиться работать с пакетом OpenSSL

**2. Ход работы**

**Проверка скорости алгоритмов шифрования**

**К**оманда – openssl speed aes des rsa.

Результат:

|  |
| --- |
| Doing des-ede3 for 3s on 16 size blocks: 7270776 des-ede3's in 3.00s  Doing des-ede3 for 3s on 64 size blocks: 1866284 des-ede3's in 3.00s  Doing des-ede3 for 3s on 256 size blocks: 454682 des-ede3's in 3.02s  Doing des-ede3 for 3s on 1024 size blocks: 116732 des-ede3's in 3.02s  Doing des-ede3 for 3s on 8192 size blocks: 14138 des-ede3's in 2.98s  Doing des-ede3 for 3s on 16384 size blocks: 7361 des-ede3's in 3.02s  Doing aes-128-cbc for 3s on 16 size blocks: 181869636 aes-128-cbc's in 3.00s  Doing aes-128-cbc for 3s on 64 size blocks: 78860353 aes-128-cbc's in 3.00s  Doing aes-128-cbc for 3s on 256 size blocks: 20134068 aes-128-cbc's in 3.02s  Doing aes-128-cbc for 3s on 1024 size blocks: 5093628 aes-128-cbc's in 3.00s  Doing aes-128-cbc for 3s on 8192 size blocks: 657475 aes-128-cbc's in 3.02s  Doing aes-128-cbc for 3s on 16384 size blocks: 328154 aes-128-cbc's in 3.02s  Doing aes-192-cbc for 3s on 16 size blocks: 178746413 aes-192-cbc's in 3.02s  Doing aes-192-cbc for 3s on 64 size blocks: 67214076 aes-192-cbc's in 3.02s  Doing aes-192-cbc for 3s on 256 size blocks: 17221139 aes-192-cbc's in 3.02s  Doing aes-192-cbc for 3s on 1024 size blocks: 4374693 aes-192-cbc's in 3.02s  Doing aes-192-cbc for 3s on 8192 size blocks: 550559 aes-192-cbc's in 3.02s  Doing aes-192-cbc for 3s on 16384 size blocks: 274683 aes-192-cbc's in 3.02s  Doing aes-256-cbc for 3s on 16 size blocks: 174372611 aes-256-cbc's in 3.02s  Doing aes-256-cbc for 3s on 64 size blocks: 57840863 aes-256-cbc's in 3.02s  Doing aes-256-cbc for 3s on 256 size blocks: 14814912 aes-256-cbc's in 3.02s  Doing aes-256-cbc for 3s on 1024 size blocks: 3734040 aes-256-cbc's in 3.00s  Doing aes-256-cbc for 3s on 8192 size blocks: 451632 aes-256-cbc's in 3.02s  Doing aes-256-cbc for 3s on 16384 size blocks: 228193 aes-256-cbc's in 3.02s  Doing 512 bits private rsa's for 10s: 265789 512 bits private RSA's in 9.97s  Doing 512 bits public rsa's for 10s: 4204204 512 bits public RSA's in 10.02s  Doing 1024 bits private rsa's for 10s: 146400 1024 bits private RSA's in 10.02s  Doing 1024 bits public rsa's for 10s: 2051734 1024 bits public RSA's in 10.00s  Doing 2048 bits private rsa's for 10s: 22288 2048 bits private RSA's in 10.02s  Doing 2048 bits public rsa's for 10s: 721505 2048 bits public RSA's in 10.00s  Doing 3072 bits private rsa's for 10s: 7355 3072 bits private RSA's in 10.00s  Doing 3072 bits public rsa's for 10s: 357201 3072 bits public RSA's in 10.02s  Doing 4096 bits private rsa's for 10s: 3339 4096 bits private RSA's in 10.00s  Doing 4096 bits public rsa's for 10s: 211698 4096 bits public RSA's in 10.00s  Doing 7680 bits private rsa's for 10s: 366 7680 bits private RSA's in 10.03s  Doing 7680 bits public rsa's for 10s: 63312 7680 bits public RSA's in 10.02s  Doing 15360 bits private rsa's for 10s: 73 15360 bits private RSA's in 10.16s  Doing 15360 bits public rsa's for 10s: 16292 15360 bits public RSA's in 10.00s  version: 3.0.0  built on: built on: Thu Sep 9 01:34:09 2021 UTC  options:bn(64,64)  compiler: cl /Z7 /Fdossl\_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL\_ENDIAN -DOPENSSL\_PIC -D\_USING\_V110\_SDK71\_ -D\_WINSOCK\_DEPRECATED\_NO\_WARNINGS -D\_WIN32\_WINNT=0x0502  CPUINFO: OPENSSL\_ia32cap=0x7ffaf3bfffebffff:0x40000008029c67af  The 'numbers' are in 1000s of bytes per second processed.  type 16 bytes 64 bytes 256 bytes 1024 bytes 8192 bytes 16384 bytes  des-cbc 0.00 0.00 0.00 0.00 0.00 0.00  des-ede3 38777.47k 39814.06k 38598.50k 39638.07k 38808.29k 39992.58k  aes-128-cbc 969971.39k 1682354.20k 1709205.03k 1738625.02k 1786042.76k 1782872.58k  aes-192-cbc 948374.75k 1426470.75k 1461923.01k 1485491.61k 1495603.51k 1492362.70k  aes-256-cbc 925168.67k 1227544.95k 1257655.53k 1274552.32k 1226866.52k 1239780.85k  sign verify sign/s verify/s  rsa 512 bits 0.000038s 0.000002s 26662.2 419764.5  rsa 1024 bits 0.000068s 0.000005s 14617.2 205173.4  rsa 2048 bits 0.000449s 0.000014s 2225.3 72150.5  rsa 3072 bits 0.001360s 0.000028s 735.5 35664.4  rsa 4096 bits 0.002995s 0.000047s 333.9 21169.8  rsa 7680 bits 0.027408s 0.000158s 36.5 6321.3  rsa 15360 bits 0.139127s 0.000614s 7.2 1629.2  F4670000:error:0308010C:digital envelope routines:inner\_evp\_generic\_fetch:unsupported:crypto\evp\evp\_fetch.c:346:Global default library context, Algorithm (DES-CBC : 11), Properties () |

**Симметричный шифр (AES 256):**

Шифрование:

1. Cd "C:\Users\Kur7u\OneDrive\Учеба\БГУИР\5\семестр\СиМОИБ\Лабораторные\Лабораторная 3"

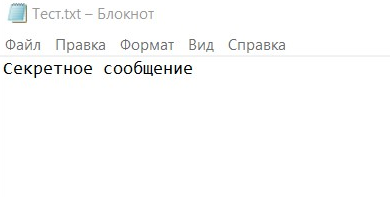


Рис 1. Нешифрованное сообщение

2. openssl aes-256-cbc -a -salt -in test.txt -out output.txt.enc

Результат:

enter AES-256-CBC encryption password:

Verifying - enter AES-256-CBC encryption password:

\*\*\* WARNING : deprecated key derivation used.

Using -iter or -pbkdf2 would be better.

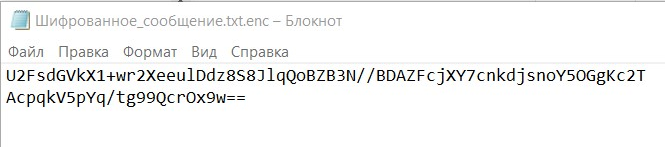


Рис 2. Зашифрованное сообщение

Дешифрование:

1. openssl aes-256-cbc -d -a -in output.txt.enc -out output.txt.new

Результат:

enter AES-256-CBC decryption password:

\*\*\* WARNING : deprecated key derivation used.

Using -iter or -pbkdf2 would be better.

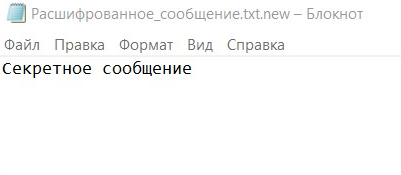


Рис 3. Расшифрованное сообщение

**Ассиметричный шифр (RSA)**

Шифрование:

1. openssl genpkey -algorithm RSA -out Ключ\_приватный.key -pkeyopt rsa\_keygen\_bits:2048

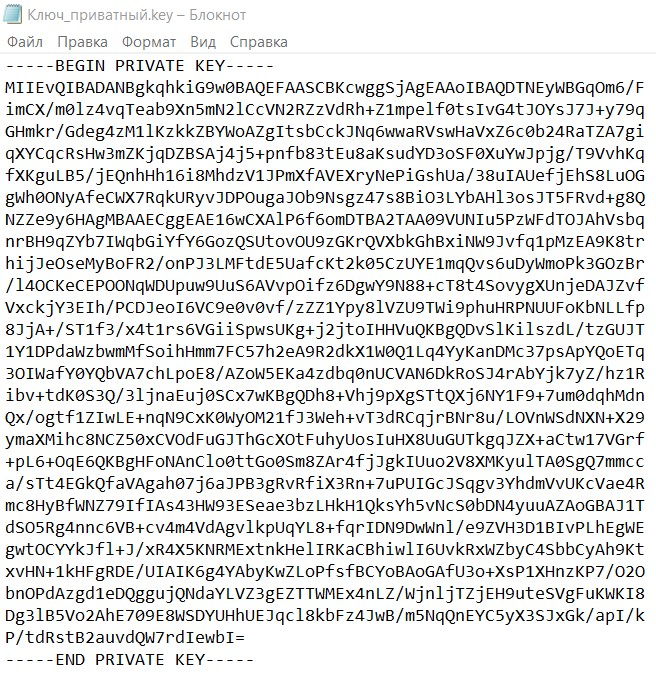


Рис 4. Сгенерированный приватный ключ

2. openssl rsa -pubout -in Ключ\_приватный.key -out Ключ\_публичный.pem

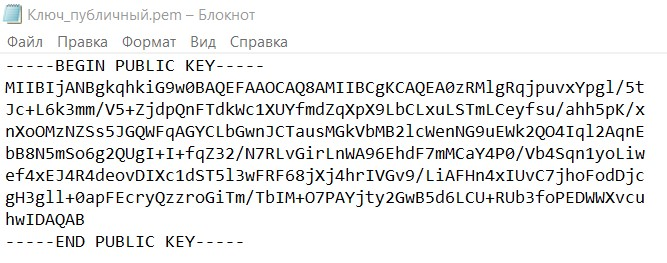


Рис 5. Сгенерированный публичный ключ

3. openssl rsautl -encrypt -inkey Ключ\_публичный.pem -pubin -in Тест.txt -out Шифрованное\_сообщение\_2.txt

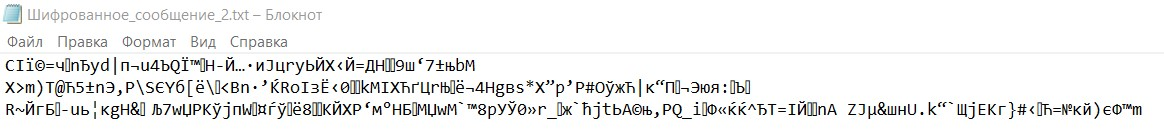


Рис 6. Зашифрованное сообщение

4. openssl rsautl -decrypt -inkey Ключ\_приватный.key -in Шифрованное\_сообщение\_2.txt -out Расшифрованное\_сообщение\_2.txt

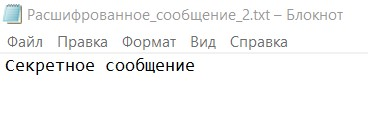


Рис 7. Расшифрованное сообщение

**Хеширование**

1. openssl dgst -sha1 Тест.txt

Результат:

SHA1(╥хёЄ.txt)= 799e274f63a5b51a7b8a9b16bf6c8a76a535c248

2. openssl dgst -md5 Тест.txt

Результат:

MD5(╥хёЄ.txt)= f3f23b2d5d0e755df0e5d3dc8f572c34

**Создание сертификата .509**

1. openssl req -x509 -newkey rsa:4096 -keyout Ключ.pem -out Сертфикат.pem -sha256 -days 365

Результат:

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

-----

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]:BY

State or Province Name (full name) [Some-State]:Minsk

Locality Name (eg, city) []:Minsk

Organization Name (eg, company) [Internet Widgits Pty Ltd]:BSUIR

Organizational Unit Name (eg, section) []:.

Common Name (e.g. server FQDN or YOUR name) []:.

Email Address []:.

2. openssl x509 -in Сертфикат.pem -text

Результат:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

3c:7c:c1:c8:c0:54:23:84:c5:94:b6:56:9d:2c:f4:0f:6d:a1:42:99

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = BY, ST = Minsk, L = Minsk, O = BSUIR

Validity

Not Before: Nov 24 07:52:34 2021 GMT

Not After : Nov 24 07:52:34 2022 GMT

Subject: C = BY, ST = Minsk, L = Minsk, O = BSUIR

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:

00:df:41:f7:26:df:3c:77:37:5a:b0:39:6b:79:76:

8e:f5:19:de:20:bf:89:09:11:dc:33:ab:5c:b0:c7:

9f:92:75:e3:44:6a:e8:cf:fc:ea:76:88:8a:b8:35:

ee:88:e2:bb:41:60:18:2c:78:b3:15:c8:10:7e:37:

b7:b3:a1:be:e4:03:cd:4d:c2:53:46:6d:8c:e3:95:

ba:a8:f4:d9:fd:09:d6:96:ba:96:39:04:a5:55:de:

10:87:4f:ea:de:f6:52:d3:30:1d:0b:b5:1a:8d:76:

3e:10:53:ae:0d:f7:b4:c8:7c:07:69:6d:fb:6f:0f:

c4:31:ac:33:dc:33:d3:f0:99:eb:5a:2a:51:97:91:

c9:52:2a:e0:4e:d2:3c:23:56:89:d2:72:2a:c9:d5:

93:4f:9c:5d:fd:7a:c6:fd:49:ac:59:6a:e6:20:66:

76:28:41:2a:fd:2d:11:30:f9:7e:24:cb:42:a1:32:

c0:fa:43:74:9b:62:7a:03:2c:6d:f2:3c:5c:ff:1e:

8d:c4:48:eb:53:e6:0e:1c:a8:3d:a5:8c:df:02:d6:

4b:c6:14:12:bd:d0:37:48:b5:bb:60:85:da:f7:55:

cd:3d:6f:eb:5b:31:c1:60:df:28:9b:e7:5a:72:a9:

67:00:08:d7:cf:f4:a0:2e:e0:06:64:12:ba:8d:52:

70:66:65:6b:b7:fe:50:0c:15:2e:ef:fa:d4:91:08:

d8:e2:a4:81:18:78:9c:20:40:2b:a0:34:59:c8:39:

76:a4:ae:72:bc:0a:f4:09:be:ba:3b:c6:dd:b4:35:

58:4f:e2:75:a3:08:0c:8f:a5:72:5c:0a:8c:92:01:

6a:b7:f6:c4:e0:41:9a:3a:94:08:10:bc:42:da:15:

95:60:b4:dc:4f:6b:11:5d:9d:df:ad:2e:07:84:78:

66:b4:42:56:ee:89:ec:a3:98:96:ca:fa:95:7d:29:

5a:63:91:be:e2:84:76:d7:8a:31:2f:1c:81:d7:a9:

c3:74:38:52:76:a5:f4:9c:35:bb:da:34:08:4c:ff:

c7:df:c0:b9:7f:83:67:d5:2d:6c:4a:0b:d0:f0:f1:

c0:b2:93:8d:8d:9d:db:38:8f:1f:d6:b3:9a:ee:0b:

2a:68:69:71:51:92:47:df:80:f3:35:20:b2:ca:85:

f2:dd:01:5d:2d:bd:21:f6:b8:30:66:7d:6a:12:28:

0c:c6:24:ee:ee:49:07:d6:2d:ca:27:a5:a3:0e:30:

43:9a:e1:09:59:0b:ec:d3:03:ec:61:72:4e:09:85:

5b:d1:32:9e:5f:78:83:8c:2c:d8:c1:fa:7c:89:b1:

73:a2:2b:cf:6a:57:8e:a3:53:0a:cb:6c:af:a1:15:

41:cb:e9

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

E2:13:4A:F8:29:5F:80:7E:DE:F2:B9:DF:22:41:40:17:04:33:09:D8

X509v3 Authority Key Identifier:

E2:13:4A:F8:29:5F:80:7E:DE:F2:B9:DF:22:41:40:17:04:33:09:D8

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

42:d2:ac:7d:0f:27:f7:30:44:e8:cc:fa:7a:49:54:4e:a3:8e:

90:2b:b1:57:1f:47:e9:33:d9:cb:f3:7a:d7:e7:0a:9a:bc:45:

f6:e3:d7:45:8a:c6:02:c3:cf:27:32:2d:6d:2a:8f:73:83:56:

90:6c:ec:cf:55:f2:08:0c:af:7c:e2:5d:e0:31:0f:a3:52:f0:

18:40:55:83:4c:ca:23:af:a7:52:5b:f2:56:3b:39:31:60:29:

39:b4:c9:38:bd:77:0e:3c:14:7c:93:16:b1:d7:4c:1e:be:bf:

36:34:1a:a4:26:c8:15:79:00:50:e9:6a:e6:6f:82:3b:a8:66:

50:50:af:0a:2a:1e:fd:af:1e:50:78:94:63:f2:a5:a5:25:ac:

35:7d:dd:f2:d9:27:0f:57:d3:b7:fb:7b:56:01:c4:9e:12:b1:

8b:7c:27:52:85:c2:4b:4f:f1:5e:28:3f:4a:96:79:f6:13:95:

ce:0f:df:92:eb:d5:89:bc:aa:22:ef:c7:2f:e2:d2:04:4e:67:

05:2b:ae:72:be:27:ee:a9:7c:9e:91:7c:e4:da:51:a1:b5:0c:

92:1a:31:33:a7:90:d3:d9:44:f7:6b:f6:8c:0b:fc:a3:f1:b3:

2d:76:41:d2:66:02:f5:27:bd:be:46:08:65:d8:44:67:c1:d7:

0d:0c:5e:b4:36:17:d5:76:82:b1:e3:56:c5:5e:b6:05:16:bb:

21:9d:1f:88:b1:f0:00:10:ad:a8:42:7e:5d:64:5e:dd:82:62:

8b:31:14:4a:89:b1:08:35:5c:37:7b:0e:87:d5:4a:87:e3:8c:

9d:a8:31:d5:0d:87:03:ca:24:9b:96:d8:74:2b:ff:08:1a:3b:

90:0e:d6:50:a1:e7:00:22:0c:6e:14:06:f2:b9:7f:fb:7a:db:

70:11:0a:fe:3f:b4:73:c9:38:b7:1e:fe:aa:f8:85:7d:a7:82:

cb:b1:b3:dc:e9:bf:ca:6a:33:b0:1e:2e:42:99:17:cb:b3:2e:

1a:fb:40:bc:79:ac:1c:9a:e4:3d:b3:33:5a:30:71:93:84:cf:

f3:d2:cf:cf:e2:98:ab:d3:75:1b:dc:11:e7:89:8b:29:4a:fd:

c1:52:f8:1d:2b:28:db:14:c8:58:b1:11:69:11:07:b0:13:82:

5b:90:df:07:91:c3:36:3d:3c:31:81:3f:67:44:10:b4:ef:75:

d4:46:ab:e6:41:00:e9:93:5e:3b:0d:ec:48:38:28:86:92:0e:

ec:e9:0c:f4:fb:c0:f5:c3:bb:d3:ba:53:0e:1e:28:b9:93:27:

2f:99:d6:44:ec:15:97:d7:60:4f:57:94:fd:64:b1:71:aa:35:

48:0a:73:bc:3e:19:20:c9

-----BEGIN CERTIFICATE-----

MIIFWzCCA0OgAwIBAgIUPHzByMBUI4TFlLZWnSz0D22hQpkwDQYJKoZIhvcNAQEL

BQAwPTELMAkGA1UEBhMCQlkxDjAMBgNVBAgMBU1pbnNrMQ4wDAYDVQQHDAVNaW5z

azEOMAwGA1UECgwFQlNVSVIwHhcNMjExMTI0MDc1MjM0WhcNMjIxMTI0MDc1MjM0

WjA9MQswCQYDVQQGEwJCWTEOMAwGA1UECAwFTWluc2sxDjAMBgNVBAcMBU1pbnNr

MQ4wDAYDVQQKDAVCU1VJUjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB

AN9B9ybfPHc3WrA5a3l2jvUZ3iC/iQkR3DOrXLDHn5J140Rq6M/86naIirg17oji

u0FgGCx4sxXIEH43t7OhvuQDzU3CU0ZtjOOVuqj02f0J1pa6ljkEpVXeEIdP6t72

UtMwHQu1Go12PhBTrg33tMh8B2lt+28PxDGsM9wz0/CZ61oqUZeRyVIq4E7SPCNW

idJyKsnVk0+cXf16xv1JrFlq5iBmdihBKv0tETD5fiTLQqEywPpDdJtiegMsbfI8

XP8ejcRI61PmDhyoPaWM3wLWS8YUEr3QN0i1u2CF2vdVzT1v61sxwWDfKJvnWnKp

ZwAI18/0oC7gBmQSuo1ScGZla7f+UAwVLu/61JEI2OKkgRh4nCBAK6A0Wcg5dqSu

crwK9Am+ujvG3bQ1WE/idaMIDI+lclwKjJIBarf2xOBBmjqUCBC8QtoVlWC03E9r

EV2d360uB4R4ZrRCVu6J7KOYlsr6lX0pWmORvuKEdteKMS8cgdepw3Q4Unal9Jw1

u9o0CEz/x9/AuX+DZ9UtbEoL0PDxwLKTjY2d2ziPH9azmu4LKmhpcVGSR9+A8zUg

ssqF8t0BXS29Ifa4MGZ9ahIoDMYk7u5JB9Ytyielow4wQ5rhCVkL7NMD7GFyTgmF

W9Eynl94g4ws2MH6fImxc6Irz2pXjqNTCstsr6EVQcvpAgMBAAGjUzBRMB0GA1Ud

DgQWBBTiE0r4KV+Aft7yud8iQUAXBDMJ2DAfBgNVHSMEGDAWgBTiE0r4KV+Aft7y

ud8iQUAXBDMJ2DAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4ICAQBC

0qx9Dyf3METozPp6SVROo46QK7FXH0fpM9nL83rX5wqavEX249dFisYCw88nMi1t

Ko9zg1aQbOzPVfIIDK984l3gMQ+jUvAYQFWDTMojr6dSW/JWOzkxYCk5tMk4vXcO

PBR8kxax10wevr82NBqkJsgVeQBQ6Wrmb4I7qGZQUK8KKh79rx5QeJRj8qWlJaw1

fd3y2ScPV9O3+3tWAcSeErGLfCdShcJLT/FeKD9Klnn2E5XOD9+S69WJvKoi78cv

4tIETmcFK65yvifuqXyekXzk2lGhtQySGjEzp5DT2UT3a/aMC/yj8bMtdkHSZgL1

J72+Rghl2ERnwdcNDF60NhfVdoKx41bFXrYFFrshnR+IsfAAEK2oQn5dZF7dgmKL

MRRKibEINVw3ew6H1UqH44ydqDHVDYcDyiSblth0K/8IGjuQDtZQoecAIgxuFAby

uX/7ettwEQr+P7RzyTi3Hv6q+IV9p4LLsbPc6b/KajOwHi5CmRfLsy4a+0C8eawc

muQ9szNaMHGThM/z0s/P4pir03Ub3BHniYspSv3BUvgdKyjbFMhYsRFpEQewE4Jb

kN8HkcM2PTwxgT9nRBC073XURqvmQQDpk147DexIOCiGkg7s6Qz0+8D1w7vTulMO

Hii5kycvmdZE7BWX12BPV5T9ZLFxqjVICnO8PhkgyQ==

-----END CERTIFICATE-----

**3. Выводы**

OpenSSL - полнофункциональный набор инструментов для протоколов Transport Layer Security (TLS) и Secure Sockets Layer (SSL), который обычно используется для генерации закрытых ключей, создания CSR (ключ, генерируемый при запросе на выдачу (подпись) SSL сертификата), установки SSL/TLS сертификата и определения информации о сертификате. Лицензирован под лицензией в стиле Apache (т.е. имеет открытый исходный код).