Kaunas University of Technology
Faculty of Mathematics and Natural Sciences

Cryptology

1st laboratory work report

Marius Arlauskas

Digitally signed by Marius Arlauskas
Date: 2022.12.09 16:34:30 +02'00'

Marius Arlauskas 2022-12-09
Student

Assoc. prof. dr. Kęstutis Lukšys
Lecturer

Kaunas, 2022

1. Task 1

Task.

Sugeneruokite 32 bitų ilgio RSA kriptosistemos raktus. Paaiškinkite kokie parametrai yra sugeneruoti ir parašykite kurie iš jų yra viešieji, o kurie turi būti laikomi paslaptyje. Matematinėmis priemonėmis patikrinkite ar sugeneruoti raktai yra tinkami.

Results and comments.

e is 65537 (0x10001)

Private-Key: (32 bit)

modulus: 3703726441 (0xdcc26169)

publicExponent: 65537 (0x10001)

privateExponent: 704869941 (0x2a037635)

prime1: 62303 (0xf35f)

prime2: 59447 (0xe837)

exponent1: 47415 (0xb937)

exponent2: 18719 (0x491f)

coefficient: 41339 (0xa17b)

Parametrai „Modulus“, „e“, „Public exponent“ yra vieši, o parametrai „Private exponent“, „Prime 1“, „Prime 2“, „exponent1“, „exponent2“, „coefficient“ yra privatūs.

Modulus reikšmė gaunama sudauginus pirminių skaičių prime1 ir prime2 reikšmes.

PublicExponent yra laisvai pasirenkamas natūralusis skaičius, kuriam turi būti tenkinama sąlyga $1 < e < \phi(n)$, kur $\phi(n) = (p-1) \cdot (q-1)$.

PrivateExponent žymimas raide d bei gaunamas $e^{-1} mod(\phi(n))$, t.y. turi būti tenkinama

$e \cdot d \; mod \phi(n) = 1$ sąlyga.

Prime1 ir Prime2 – saugūs pirminiai skaičiai, žymimi p ir q.

Exponent1 – sveikasis skaičius, kuris apskaičiuojamas $d \; mod(q-1)$

Exponent2 – sveikasis skaičius, kuris apskaičiuojamas $d \; mod \; (p-1)$

Coefficient – parametras, gaunamas $q^{-1}(mod \; (p))$

Tikrinimas:

$$p = 62303$$

$$q = 59447$$

$$n = p \cdot q$$

$$n = 3703726441$$

$$\phi = (p-1)\cdot(q-1)$$
$$\phi = 3703604692$$
$$e = 65537$$
$$d = mulinv(e, \phi)$$
$$d = 704869941$$
$$exponent1 = mod(d, p-1)$$
$$exponent1 = 47415$$
$$exponent2 = mod(d, q-1)$$
$$exponent2 = 18719$$
$$coefficient = mulinv(q, p) = 41339$$
$$\gcd(coefficient, fi) = 1$$

Tikrinta su Octave.

2. Task 2

Task.

Sugeneruokite 2048 bitų ilgio raktus ir sugeneruokite sertifikato užklausą (naudodami CryptoGen įrankį). Laboratorinio darbo atskaitoje pateikite TIK VIEŠĄJĄ rakto dalį (Nepamirškite persivadinti ir saugiai išsaugoti sugeneruoto raktų failo).

Results and comments.
Private-Key: (2048 bit)
modulus:

00:bf:d6:aa:47:cb:be:ea:44:8b:66:ae:69:c9:74:
66:11:76:5b:ff:24:98:10:60:a4:3c:fe:ea:d1:f8:
74:6d:05:38:f8:df:a7:38:00:03:c5:75:bd:cc:47:
90:6f:9e:b7:f1:b0:c7:dd:7b:a5:ec:3e:91:83:5b:
3d:1a:0c:a9:40:c7:f9:c5:d7:d2:b5:02:dd:fd:33:
18:17:d1:11:14:0e:67:82:1a:d2:91:62:fb:0e:67:
35:3c:41:bf:d9:65:f4:00:7f:c9:5f:ed:ec:95:54:
20:8e:0a:6d:dd:f2:a2:78:02:71:b2:91:5c:ab:85:

05:75:a2:b1:08:b9:78:da:7e:d1:a0:ac:58:c8:31:
c1:bc:02:db:0a:ce:9b:16:c6:f9:8a:64:4b:12:0d:
88:14:4d:e2:af:37:5d:6b:91:e1:24:71:19:5a:e3:
12:91:5f:7a:0f:49:e4:d4:73:96:06:85:8a:10:93:
48:07:9e:e1:8b:46:4b:61:ab:8c:06:d7:f2:b2:6a:
84:8c:51:31:c7:88:ee:3f:ad:90:ec:72:c9:58:36:
86:ea:e3:fe:d8:3f:c8:1e:b1:ab:d9:e5:8a:c2:3a:
3b:60:f9:4c:12:64:1a:4b:34:1c:3b:52:cf:3c:ba:
95:35:43:ca:7e:82:00:b3:9c:8c:30:b9:4b:6d:f1:
0f:29
publicExponent: 65537 (0x10001)
privateExponent: privatus
prime1: privatus
prime2: pivatus
exponent1: privatus
exponent2: privatus
coefficient: privatus

3. Task 3

Results and comments.
Certificate:
Data:
Version: 1 (0x0)
Serial Number:
92:ea:df:10:d7:27:30:28
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=LT, ST=Kaunas, L=Kaunas, O=KTU, OU=TMK,
CN=CryptoCA/emailAddress=kestutis.luksys@ktu.lt
Validity
Not Before: Sep 26 11:19:12 2022 GMT
Not After : Sep 26 11:19:12 2023 GMT

Subject: C=LT, O=KTU, CN=Marius Arlauskas, GN=Marius, SN=Arlauskas/title=Studentas/emailAddress=mararl1@ktu.lt

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (3072 bit)

Modulus:

00:cd:08:b3:bb:b1:b6:15:1f:40:b8:71:3f:0d:cc:
24:80:ba:a4:cd:ce:cb:fc:f8:31:e9:08:72:06:52:
43:6d:be:93:92:0e:45:2c:4a:d0:7c:d4:21:60:e9:
df:e9:15:2f:51:5d:2c:ee:a8:51:3d:b4:65:af:39:
2b:59:72:70:1c:2f:e8:d3:65:b0:42:f0:01:82:72:
75:7a:26:01:b3:94:63:91:e1:5b:e9:40:e8:e4:f7:
04:02:82:98:ea:6e:e2:92:5d:c5:e9:73:57:74:32:
23:64:b4:66:cb:53:e8:11:0f:ab:5d:11:10:89:f7:
bf:f0:62:cf:08:d1:59:2d:8d:a5:c0:50:af:3c:8b:
79:1c:64:12:a1:65:fc:14:06:07:aa:5d:25:77:87:
59:fc:d1:9f:7b:b7:05:9e:f2:ec:25:c9:fb:41:5e:
bd:73:e2:6a:ba:ff:3d:09:99:97:52:d9:b5:c4:79:
68:b6:45:84:a2:68:cc:28:13:ad:4b:e2:60:f9:7b:
c6:05:26:08:9e:3e:ff:2a:98:aa:e9:a7:10:94:a6:
5f:ec:61:aa:7a:d0:21:f3:75:63:72:d4:ff:b3:e8:
cd:9f:45:0c:71:89:c6:39:2c:90:3f:c5:cb:d6:e9:
5b:19:5b:26:25:9f:b8:ff:3f:58:2b:b9:2b:08:e9:
43:5b:c8:dc:2e:f3:a9:83:1c:12:8c:60:86:67:eb:
0e:de:40:40:af:5f:88:34:7f:12:5d:61:42:8d:4a:
60:ee:67:e3:44:d8:0f:34:a7:1f:04:49:d3:44:01:
67:6a:d0:27:bc:fb:d2:4b:96:b8:d4:a6:11:a3:47:
bf:04:b4:7d:f5:91:b2:a4:7e:6b:0c:44:43:9b:78:
27:84:2c:bc:15:ec:fc:e3:55:98:81:52:5a:97:25:
af:1a:4c:3c:fe:c8:09:0b:92:7b:41:dd:1f:33:89:
84:f3:77:79:22:77:a7:b8:ea:8b:d2:92:6a:91:f9:
4d:37:a2:37:8a:a4:6e:63:88:47

Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption

89:ae:2d:13:52:74:4b:69:32:bb:d5:5c:80:f5:01:26:5c:62:

d3:9e:41:28:82:53:e6:3a:84:83:50:8f:fd:34:dc:28:11:3b:
da:81:b9:2d:a3:b4:50:ec:6d:41:9a:34:b6:42:86:66:98:42:
b5:1f:9b:60:00:79:df:a8:ad:80:15:fe:73:fd:94:72:0a:13:
bd:45:25:00:c8:5c:6d:c6:1a:f4:4d:10:b5:2a:3d:88:2f:75:
6b:2d:a5:66:06:59:00:62:74:87:1d:16:d7:a3:5d:40:6c:00:
e5:5e:15:1d:6b:ee:8a:c6:b2:ea:b2:31:17:0d:55:b3:da:ea:
59:b6:93:ae:58:18:04:5e:c8:4e:4c:56:40:01:4c:b5:01:e7:
48:0f:b6:ae:bb:b9:07:38:dd:c2:47:82:14:b3:29:d7:41:c2:
c8:1d:fb:d0:b4:79:43:27:5d:8d:2c:3e:0d:02:9a:d5:23:c8:
68:ec:a9:5e:aa:e1:93:95:ad:d0:f9:ff:94:32:ef:79:f3:a4:
82:9b:d5:c6:d2:8b:7b:cf:cc:0b:20:94:1b:aa:79:8a:74:32:
83:2d:af:96:1d:b5:23:06:de:a1:9b:34:cb:84:f2:a0:7a:81:
31:09:b8:73:29:ab:1d:8c:6e:6f:f8:14:97:d9:45:c4:ea:49:
e4:b4:4b:75:5d:23:65:28:38:a9:5a:0b:b6:bb:f3:cc:d0:5d:
a2:64:b6:8e:09:2c:15:52:8f:0a:ae:69:e3:30:c3:0f:ca:59:
17:c6:1d:5d:8d:0e:b2:f6:86:00:7f:5e:a4:32:00:c6:cc:5b:
91:04:5e:ca:b4:dc:d3:26:2f:84:2e:11:bf:7d:41:f2:ef:96:
c8:b5:76:1b:27:5f:f5:ac:b7:d4:5e:07:1b:fd:6d:8d:a9:6e:
a9:61:bf:36:63:c9:3d:57:66:24:8b:ab:ac:b1:88:c6:16:e4:
4a:43:82:24:0d:f5:1f:1a:86:f9:71:76:c1:81:a1:cb:46:a0:
48:e4:0d:6c:39:80:e9:59:e7:44:3f:42:0b:b6:0a:2f:56:9b:
13:18:3b:ad:48:88:95:30:7f:fc:c5:fb:2a:0a:9b:ec:dc:d7:
f3:09:2b:16:38:69:2c:44:74:8b:d4:20:bc:4e:d5:ac:8b:13:
80:79:2e:68:c9:c7:b8:c6:6b:02:71:dd:b2:1a:32:22:54:f6:
32:70:43:a9:af:47:19:bf:0f:6a:82:43:ba:ad:92:69:20:c9:
91:4a:aa:d3:59:32:0e:e3:af:20:4f:f1:b2:38:e2:9b:48:b1:
a0:3a:3b:33:e4:aa:3e:55:b7:cf:1f:2e:34:3e:3a:a1:8a:9e:
47:bd:43:1b:7b:6b:7d:9f