Lab10

sâmbătă, 6 ianuarie 2024 13:12

1)
N=234841136411758273000763594354834942653
e=65537

p q

- 234 841136 411758 273000 763594 354834 942653 (39 digits) = 14 086963 408384 851001 × 16 670813 262138 239653

q = 16 670813 262138 239653
p = 14 086963 408384 851001
phi(N) = 285294448034526419904389331861504000 → (p-1)(q-1)
d = 65537 ^(-1) (mod phi(N)) = 69784787574089079813210254551686272348

ex.2 openssl genrsa -out alice_sk.pem 2048

Rezultat:

```
Generating RSA private key, 2048 bit long modulus
............+++
.....+++
e is 65537 (0x10001)
```

- exponentul de criptare: e = 65537

openssl rsa -in alice_sk.pem -text

fisierul meu are continutul:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA0CUNDX8JpRKaIqKtCX4QuRuNDyUDB769rjP5flCc5Wh4Ey63
eI8enV9tx0Oa4d2esN62YjFHVw8Jgv9Qm+DAPkp41ldOwXqExM1GxfQvRDPeOvaS
7bd5MwL2DxF/boXXbTDM03l0UwqO468nmhLZXlhmpmzVDUzklLDmrxFcUzqd3IDi
UGHNElTTk/jBkyFtU91bmbZm0fd5R9UiMTgCzAjOZWudPabqRBj9girg9M5djM8c
GRxpSkt9tnfnZfe3OmRLKqQ8nLU9yqtmEP6ebhLuHgzgIwIm95fSwqVifzx+K8G3
lHgx2LKCzTi3ErdfimTcOXmnH1HMoNGFA+z5iQIDAQABAoIBAQCqQVRO8NYLz46C
vDv8IsE9GLsmYyj6Ydw3rU3sM7ZStERbtH/gvnjVU2SxdKwxCp2uoU3gPdzT6nnm
TD88cffuO+5hrSK/gh8t95dnfphXGnIyGtUOW2BpClgKxU5OMm6HYz530MYE0wMU
XIZxMe/Zi0fT4/vVmEr1EUpwcyvo6vQMFt18y73KyQmqCyzOoCgezK05ooi2Oj9x
xmajgk6oZe8Rbkr5L29BBsrkFUvYWM5Di2GGvSZ/Be2m3mRbUJ6aDSnHZ/ItaB+q
AjQX+jz4H1fy/oDAYBbFfzxfUK7yp1Win/CJ/XiJrkLYBYpYk10g7NfVbs3nS/0Y
xrtrtBYNAoGBAPb1/4t1kPlzNqcrYYRA/plysOn4RewZjIewRXRX8UrbLcIKIChe
5vnMoUU0fikLaQZ9+MY8mcLcyLXBWLI9xI06ZEKaxESIccn74tE8577XUL3tqjJP
FGeOAOpvfDjq7De0F0ScFJCdeAf+CMFEOxLP1TZ8MvtdGdTai7AVf3mXAoGBANfD
WTQIkFrKGR+l5jyLG54ssIKVB20mSats8gm6zdciwvQjajpW4Bre8WBG/POsiKlX
xTNZKXFWd5Hclc+PTFOYnJz7ULc56rWA7Kod5J8A3SGZJyTlV0ah8fBK4nSGPSSr
5IXrdjzF95PJ4UNWEWp+N9T8nrXahFENs2A8OknfAoGAYUNDUNaNsWDp7m7Majz6
yM591Lf+Od1aFnqa8BZOps+pttksDxpJV6p6/XmOEnY29+KXHuPxHui7d7HdT925
```

```
0nFj2UOA9wjR393/V67oCqZcW2EF/ehdPeeUfsBHqVcEj2+zFkduZgJOqr8nDY7k
wSTvcRT7MzpYmRc1mrTszqMCgYEAuhBYKKsJ8YE+0S/7sFI16t2XCcUCtnnCJfa5
cvKI9/GeNXMk9FJeyE1h0ijlki1DXOW3xWQqfPaX/k0/U9K7e4ur4yRGovtrEEKx
1LIaqZPRHlw4iXTNIrgdL58kUmBA8hLZ6zL2r8n4ipYZkDv0oOVfuGhxZVmfqVYr
Td4iVfkCgYEAmioS0dz71s4LPAEHQPGuliUCxZCt6WsJuUhAcAR7Ybt9DPAhiR3k
oVEI6FFLsQs9rwS2liylbbxiN2LFiEjcuqrKhew2Lm6E8521uOmg2Bx81kjvPfR3
aYgps2q9Z5w/T3cERc/jL0ukEpjqkGkW4yKtYyeV9z4hA6CYQoYTQLc=
-----END RSA PRIVATE KEY-----
```

```
--
modulus:
    00:d0:25:0d:0d:7f:09:a5:12:9a:22:a2:ad:09:7e:
    10:b9:1b:8d:0f:25:03:07:be:bd:ae:33:f9:7e:50:
    9c:e5:68:78:13:2e:b7:78:8f:1e:9d:5f:6d:c7:43:
    9a:e1:dd:9e:b0:de:b6:62:31:47:57:0f:09:82:ff:
    50:9b:e0:c0:3e:4a:78:d6:57:4e:c1:7a:84:c4:ab:
    46:c5:f4:2f:44:33:de:3a:f6:92:ed:b7:79:33:02:
    f6:0f:11:7f:6e:85:d7:6d:30:cc:d3:79:74:53:0a:
    8e:e3:af:27:9a:12:d9:5e:58:66:a6:6c:d5:0d:4c:
    e4:94:b0:e6:af:11:5c:53:3a:9d:dc:80:e2:50:61:
    cd:12:54:d3:93:f8:c1:93:21:6d:53:dd:5b:99:b6:
    66:d1:f7:79:47:d5:22:31:38:02:cc:08:ce:65:6b:
    9d:3d:a6:ea:44:18:fd:82:2a:e0:f4:ce:5d:8c:cf:
    1c:19:1c:69:4a:4b:7d:b6:77:e7:65:f7:b7:3a:64:
    4b:2a:a4:3c:9c:b5:3d:ca:ab:66:10:fe:9e:6e:12:
    ee:1e:0c:e0:23:02:26:f7:97:d2:c2:a5:62:7f:3c:
    7e:2b:c1:b7:94:78:31:d8:b2:82:ab:38:b7:12:b7:
    5f:8a:64:dc:39:79:a7:1f:51:cc:a0:d1:85:03:ec:
    f9:89
publicExponent: 65537 (0x10001)
privateExponent:
    00:aa:41:54:4e:f0:d6:0b:cf:8e:82:bc:3b:fc:22:
    c1:3d:18:bb:26:63:28:fa:61:dc:37:ad:4d:ec:33:
    b6:52:b4:44:5b:b4:7f:e0:be:78:d5:53:64:b1:74:
    ac:31:0a:9d:ae:a1:4d:e0:3d:dc:d3:ea:79:e6:4c:
    3f:3c:71:f7:ee:3b:ee:61:ad:22:bf:82:1f:2d:f7:
    97:67:7e:98:57:1a:72:32:1a:d5:0e:5b:60:69:08:
    88:0a:c5:4e:4e:32:6e:87:63:3e:77:d0:c6:04:d3:
    03:14:5c:86:71:31:ef:d9:8b:47:d3:e3:fb:d5:98:
    4a:f5:11:4a:70:73:2b:e8:ea:f4:0c:16:dd:7c:cb:
    bd:ca:c9:09:aa:0b:2c:ce:a0:28:1e:cc:ad:39:a2:
    88:b6:3a:3f:71:c6:66:a3:82:4e:a8:65:ef:11:6e:
    4a:f9:2f:6f:41:06:ca:e4:15:4b:d8:58:ce:43:8b:
    61:86:bd:26:7f:05:ed:a6:de:64:5b:50:9e:9a:0d:
    29:c7:67:f2:2d:68:1f:aa:02:34:17:fa:3c:f8:1f:
    57:f2:fe:80:c0:60:16:c5:7f:3c:5f:50:ae:f2:a7:
    55:a2:9f:f0:89:fd:78:89:ae:42:d8:05:8a:58:93:
    5d:20:ec:d7:d5:6ee7:4b:fd:18:c6:bb:6b:b4:
    16:0d
prime1:
    00:f6:f5:ff:8b:75:90:f9:73:36:a7:2b:61:84:40:
    fe:99:72:b0:e9:f8:45:ec:19:8c:87:b0:45:74:57:
```

```
   f1:4a:db:2d:c2:0a:20:28:5e:e6:f9:cc:a1:45:34:
   7e:29:0b:69:06:7d:f8:c6:3c:99:c2:dc:c8:b5:c1:
   58:b2:3d:c4:8d:3a:64:42:9a:c4:44:88:71:c9:fb:
   e2:d1:3c:e7:be:d7:50:bd:ed:aa:32:4f:14:67:8e:
   00:ea:6f:7c:38:ea:ec:37:b4:17:44:9c:14:90:9d:
   78:07:fe:08:c1:44:3b:12:cf:d5:36:7c:32:fb:5d:
   19:d4:da:8b:b0:15:7f:79:97
prime2:
   00:d7:c3:59:34:08:90:5a:ca:19:1f:a5:e6:3c:8b:
   1b:9e:2c:b0:82:95:07:6d:26:49:6c:f2:09:ba:
   cd:d7:22:c2:f4:23:6a:3a:56:e0:1a:de:f1:60:46:
   fc:f3:ac:88:a9:57:c5:33:59:29:71:56:77:91:dc:
   95:cf:8f:4c:53:98:9c:9c:fb:50:b7:39:ea:b5:80:
   ec:aa:1d:e4:9f:00:dd:21:99:27:24:e5:57:46:a1:
   f1:f0:4a:e2:74:86:3d:24:e4:85:eb:76:3c:c5:
   f7:93:c9:e1:43:56:11:6a:7e:37:d4:fc:9e:b5:da:
   84:51:0d:b3:60:3c:3a:49:df
```

```
openssl genrsa -aes256 -out alice_sk.pem 2048
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,60F04F574D5E2789252D741FFE04E310

JqaV8TE5SxEt+crVq0mEsLfMULtfy3cXqi/aEQ+mhafRhS5U5f51fEh4A7ZUGFzZ
8qD/CapyChRMQQu4WPBSPMlqKXHBHAubSzKUjbyHXcwgG3MSi9vnZG8GblVU7BUx
jDGWKrTyx8GP4RLCwcZ9n1upsE9nu2nVxVs4kOKUuHPYWb2l3da8l0ELxzNX1Pj2
5G7zOIH9rYn/3WW+m+EHI1RNZMhJmguS1vIJq+Vwfzilf1uLgoxGFpVf8DkwD+Wd
193dl4fUskMSahZrew8I5hXZeYkZt2gpodavbbqXa88rM4iZEazUhDNAHjKoPeqP
NtgwVfQYqOnoo9AtWCGZbWEf+uDYSxuT9C3IHPaVkcMuPZKaJ0975rS3J5RN9NRM
bMi+ADoAM2dFoPnxIPdyBTsfi3NEK+SmTGbwUb+LDmORA2/cxSxtAEzDdkncVvTW
grg/S7CjqR2/Eb81RuyW8/9CrPLOOLuHOUQywypxBnlVDlmGDBNQA1qRysrSAy9H
A9YpH0vZhZpkLVpOYIGLbZqs3z2mo1Jc+UVnFg1fbDp/Hxk2YvETsfFxclmD4FGv
8otqgqHLIyYQsdChNOcgy9uUn1r8o4cTmE1BT8u9+8Hk1FToJbG1WQk+VhT1z18T
1eKADmC/4FTItiUNBUvDQ7iaoQ394wptTKhNLU8GnEoW6/lWnjQgs4bs5gEdzTiB
+YWG7cGZMG44Bbo9coGaQBRyM0pfGgDKmB6UOqboHNowSO+SGKiyoBG1M7yuJVLU
FKuxHLz7oBb/ik5sJEJIQKYR3oulJnZrN7SwIteVWMx4961q7diRORTT8Qk0a1Io
HeG2EpcoNncby6pb2YCp/eNPj0sqEXxZ8s9+gASV0qt3XPRrUKUW98N71QofK1w0
ZBoW01fKVzhPEWaFoRuIKLjOYNh8zg3J0nwm6hSXDs5yKCjwgyZdOu3YtNlD401R
kzSUlvI7wjZLDoc/L+wT98rpN8Ma5Yya8uJY+OH9lrng/qtWBZsk1t8+BxDuCSMf
AyHOTe6HaLLh+x51gwEExASd9FeEYra5Vyc0Z/08UPhXd5oNc2hM48caryBCxEhc
A7d2nMFy0Ho8taumoTgsQmdeVRhptL6e6bF+qEORDGoG0SkafIMpo6dyQ/w2UA3v
gyYxqF21Z9jnfsg7g/BKrDr2qVtLSsLahd4geBRD4zXviuRFikpolh0y6wuCo4ZT
QTsPGLmZpDbjx9yXPOtsuyfRjJOWw+lM7wmhHeVs7/wRKOzuC2QKcidMsV3y38dh
qnCaMZokwnStRNl9PxVbZ+3h+RV4t61dY48dqxbapi94Ee70jLPNUpr5i1x6LHQT
ZjveZEJ4CXn+G/kdn0nhsKE+g+x1ZuQNIroJGNkCt58lFrqcKd2GWfV6R7WCVMor
ylqSWGjdJwQpOjiP2TAQ1KTsn0dsjI9fzGrcDAGYm+oIpR6PecMm85RnFk4PZaGG
oDSnd5rzGqmuAkjktDfVii8BnGjBYsvFGIAgF7EJQs5VpWzUKghcGzBa1ornM3sW
3nqX75IApU9fzBs4d+mP/4o1pIqdcf+L+klRKuZP1GzANmwYofRY3BLiz+kwlvn0
```

-----END RSA PRIVATE KEY-----

parola masina123

exponentul e e acelasi pentru ambele si daca ar fi acelasi si fisierul atunci ar aparea o problema de securitate

```
openssl rsa -in alice_sk_protected.pem
```

public:

-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAsxBIUUJIysX8d0fyp9/JgdZBE00mimKIp6KLQNYxRabrHxD9d1MK
sYNnKERldbeMCZNlCptd8Cd3aeyOD9pT4DvaEID9kYmOTaTKa9LWVUYFSN91Jxwf
qgmeKATWCbmmRUSL0l5r4eXNL/WYYfQQPN0IAgLoHApuUHfHAPltL9+FWwrZZenw
Qt0SOIuzcA7NJAIqhRt+9pitw4zCdkr1PCCe6H8f6hNxyhHSL2kPlOXagIGQoId5
d3XJ4atcg4WtwyS967XFz9rFMA5KHnFP+uNweI5NNrkcPdYvxdT2676REjfhI5Un
E+yDjj0rbs+ssa7h0B5a0Fpeo34+gbUbMQIDAQAB
-----END RSA PUBLIC KEY-----

--

-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAsxBIUUJIysX8d0fyp9/JgdZBE00mimKIp6KLQNYxRabrHxD9d1MK
sYNnKERldbeMCZNlCptd8Cd3aeyOD9pT4DvaEID9kYmOTaTKa9LWVUYFSN91Jxwf
qgmeKATWCbmmRUSL0l5r4eXNL/WYYfQQPN0IAgLoHApuUHfHAPltL9+FWwrZZenw
Qt0SOIuzcA7NJAIqhRt+9pitw4zCdkr1PCCe6H8f6hNxyhHSL2kPlOXagIGQoId5
d3XJ4atcg4WtwyS967XFz9rFMA5KHnFP+uNweI5NNrkcPdYvxdT2676REjfhI5Un
E+yDjj0rbs+ssa7h0B5a0Fpeo34+gbUbMQIDAQAB
-----END RSA PUBLIC KEY-----