Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

Creative Commons

Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

OpenSSL

- OpenSSL
  - biblioteka kriptografskih funkcija razvijena u programskom jeziku C
  - alat temeljen na biblioteci
- Primjene
  - alat za izradu sažetaka, (de)šifriranje, stvaranje ključeva, potpisivanje, certifikate
  - implementacija SSL/TLS protokola
  - zahtjevi za potpisivanje certifikata, (samopotpisani) certifikati
  - Platforme: Linux, Windows, Android, MacOS
- Open source
  - OpenSSL (Apache) licenca - slobodan za nekomercijalno i komercijalno korištenje
- https://www.openssl.org/

Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

Stvaranje sažetka

tajno.txt – datoteka s tajnom porukom

openssl — -bash — 102×44

```
igor:openssl igorcavrak$ ls
tajno.txt
igor:openssl igorcavrak$ cat tajno.txt
Ovo je tajna poruka koju smiju pročitati samo odabrani!

igor:openssl igorcavrak$ openssl dgst -sha256 -out tajno.txt.digest tajno.txt
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat tajno.txt.digest
SHA256(tajno.txt)= 5a65b1c82e64b9ca859abc930564327ba0a167b66739dc9b1ea8d466bef0b895
igor:openssl igorcavrak$
```

-out *izlazna datoteka*

ulazna datoteka

dgst - sažetak

konkretni algoritam za stvaranje sažetka

Base64 kodiranje i dekodiranje

```
openssl — -bash — 102×44
igor:openssl igorcavrak$ openssl base64 -in tajno.txt -out tajno.b64
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat tajno.b64
T3ZvIGplIHRham5hIHBvcnVrYSBrb2p1IHNtaWp1IHByb8SNaXRhdGkgc2FtbyBv
ZGFicmFuaSEKCg==
igor:openssl igorcavrak$
igor:openssl igorcavrak$ openssl base64 -d -in tajno.b64 -out tajno2.txt
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat tajno2.txt
Ovo je tajna poruka koju smiju pročitati samo odabrani!

igor:openssl igorcavrak$
```

-out *izlazna datoteka*

-in *ulazna datoteka*

-d = *dekodiranje*

Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

Šifriranje tajnim ključem

```
openssl — -bash — 102×44
igor:openssl igorcavrak$ ls
tajno.txt
igor:openssl igorcavrak$ openssl aes-256-cbc -in tajno.txt -out tajno.txt.bin
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
igor:openssl igorcavrak$
igor:openssl igorcavrak$ ls
tajno.txt       tajno.txt.bin
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat tajno.txt.bin
Salted__q)?!?e|?/???E?ç$*m???a=8??ú.??2}??a??:q???n#??W??D k???igor:openssl igorcavrak$
```

2x unos šifre (ista šifra za šifriranje i dešifriranje) !

korišteni simetrični algoritam

Podržani algoritmi tajnog ključa

openssl — -bash — 102×49

```
igor:openssl igorcavrak$ openssl list-cipher-commands
aes-128-cbc
aes-128-ecb
aes-192-cbc
aes-192-ecb
aes-256-cbc
aes-256-ecb
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
chacha
des
```

Dešifriranje tajnim ključem

```
igor:openssl igorcavrak$ ls
tajno.txt       tajno.txt.bin
igor:openssl igorcavrak$
igor:openssl igorcavrak$ openssl aes-256-cbc -d -in tajno.txt.bin -out tajno2.txt
enter aes-256-cbc decryption password:
igor:openssl igorcavrak$
igor:openssl igorcavrak$ ls
tajno.txt       tajno.txt.bin   tajno2.txt
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat tajno2.txt
Ovo je tajna poruka koju smiju pročitati samo odabrani!

igor:openssl igorcavrak$
```

-d dešifriranje

Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

Stvaranje para ključeva

openssl — -bash — 102×40

```
igor:openssl igorcavrak$ openssl genrsa -out keyA.pem 2048
Generating RSA private key, 2048 bit long modulus
.......................+++
.............+++
e is 65537 (0x10001)
igor:openssl igorcavrak$ ls
keyA.pem        tajno.txt
igor:openssl igorcavrak$ cat keyA.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAu98S6eSWgpSj3jbEYei85DJGRvvvw3tEJxRDGW3gJXKVIjy
XNCATKfX34w8GL0Q08+bnOUNza8hhDf5s0kdjEmxumR7l/3H0NveONVi1MIT3YI6
XYPmIrkyYp+u8H1F+Gp7CJjBhBe+Ssr9lNcsLwfXnU3ziWdIVFBGJoDp/FjQpOhF
1Y5U6N5MrcEmfm0YkGpkB+HeCI5BPpZeV3vukn3G+oVz077ovl3whnc0WKzWNEE2
nGzCIHHD9MMyW2Rnblyi2wHk1kj3KU30JWlOwBxqtpSEpcz8ipSHQCLAk15MiH14
i4RgbfxoCcx/qUIcqJ0H06KqYqzEN8MQwIURvQIDAQABAoIBAE8ryKqsXAkXXp85
cUHZdJCt5xMPdzZsRfT0Cuuwic40UZmiRJB8hTTInp5kWIcMVeUM3kUV+eUt4m/3
rtCxBTSzcaRc6ACgR25q2ZEVy5phV0HHuZTjGr6TUPpi1LQf9rajGMocpaBm6RhX
xtlMfCAtq91sli7XSZHOaLIVLYXbpnu+S0e6vyH8ILJ3gjIB23+v9LXpxYzFI6Yg
R8/Br4bMsaV30dhCQib3Aw/MJNkVY5iQK+f/m2guPABKx5dsSmv2mpLSVJMROxsY
ZwhRKBNCb3wSNUHHCfDbf3PK3CKix0z2+hhgs7N9DmG4bufL8IPmlEcvKRXgJrBX
93N/W/kCgYEA6tq7OBhDJdPQwvNcn3UNobiQDDMnQ+9y/pso3AhEJDKyVdYIy8oF
Ybr4K+xtFdhmeVLXGy6j814Kd6nSASR4KIOh8Hp6h1RozOX4qnVYP5MwtRo81VXj
K5nhEEKcmSjDVgBNzTjH1P2f4L5eKDfEEsvhx3intfL/hDNZxG3LDq8CgYEAzMlo
oJouZ2oT8jAS84w31U0+nWhdunYlP63UHvXnSKxk8A53zj7RgzhVRLI4pSeCejDH
0MptLTv288QQ/LFVo6wKaG6JHQ3YGWPMgjSUPCo1mPa9YB2BCdYVsrp3hxSYFvRg
BtX7joh5IoLtmn7VExPRcMMPtzGK1k4ro/qRYVMCgYB2TpV9XouE5L0HV/zSvu6N
ByJZYvNmv5rYM2VT4j4hVgCMSPPJZQ1s+/jEd6dEF+0XNOnzYX1pvXfcbAnEVZDK
J/VN5QUQYy8f+MFZbR91dzpUINGATnHPpwa/YC7u4J/2FNUcinvwCYuedYeNDvqQ
1W/5QgiKGc0p1Yxk7UIbNQKBgHxbDgsAtY8c7nHSWZ/FlR4VIyHI/6m8FtB9iWMn
pkQOU9kmoAABS47ohXcK1rULsgLrXlteoT+nu0W52SrpsPyL+2IBRYf8IS8B2G10
6lNCunth0gvsvrAvbcuzyeOgUN8XlLxx8qlSHGUlpo172X4VOcjE2uU+03Vh0MRp
4yB7AoGAPcHeqBgGayVltC1A1cNJBEZvV5g2D7E91xVXyz01+k3zk0zY7KBjzV3r
8ZM0w9frYZChAzb1yV8LjG8ELJEOfVdfHwc2fpz30+7bb7Oui9JxpTL47AIc00nE
vBbd+2vwqDPIih1AMGAuMiQrivZ82T++9A+BrHrwIx6p44buweo=
-----END RSA PRIVATE KEY-----
igor:openssl igorcavrak$
```

dužina ključa

koristi se RSA asimetrični algoritam

PEM format zapisa ključeva

Problem: privatni ključ nije zaštićen !!!

Štićenje privatnog ključa

```
openssl — -bash — 102×40
igor:openssl igorcavrak$ openssl rsa -des3 -in keyA.pem -out keyA.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
igor:openssl igorcavrak$ ls
keyA.pem        tajno.txt
igor:openssl igorcavrak$ cat keyA.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,3B15A44A0CA278CB

T592R+rv3jKQ2chcBB37oS[illegible]ivSrfBr7wZsfwuuWztGCIxzU9V3HROMK9p2
s7vTKIT/AmZjyrF/AjpZcTseibJOENF[illegible]TEe07fXFh8a2QyTC92jDoLpcPq5QQ
vZL+GqArazD5cRXLWl2tprpmWh7Ywnb4jbiNL[illegible]ZH6XHWZdUwqqCgPPU18BNz
wXNOmYnfSD6cnwHvIP+p2ghnd07kljpCrPI7gR+4NAF[illegible]Fqd94sTNjH7KqQncD
LKPF/OMW4ooiCb1ZVAa25uSzwO31Y69sKyX4GV/6HWhu6u6L[illegible]GxtP9bR+BuW
cbGloPM5+f9xSbnu9UWV6Jc5Sep+PCcqBn99AflFDx8XVzjm0g8lGTI[illegible]hWQB
onanLF0uzUE1Vj5NoD78nu+9UTRy6oPB9MfnxQg2iLSxbUv5tIZ+1RtGZGsBjP[illegible]
nqqI8waCPvW1xQZSlAbJO++2IsmsgwwcB99MzFs+Rvvb4kFvc8SzOkS8qBqdS+Wt
61wac5qfTmpCZx1SD/DbhavHcex6EYTl57ZnD88pCiuNN2zEo/JJuZiuf68E3gQT
wphPxt8k7cSysnOZLpOVZ0yCAfz8NC1stMA5/E89Stq4/xnH+Epkysz5Ry/Cl8Gq
RQ6iTk1j7L9TMdPoER+DrOCJQPAhBbtUdJ/u/E9UbvvzKtoUSPTyA9y3JXcsTlyG
Ur4tnCRqS6mNmoKHHWtIsr8khm5WIbwdOJ00B5CmDOw2LO/isnfb4sTrkP8XDYKo
UtofMHNKDtfgUTHbz1O3NjWJRui1a9OboZwKpaKGn5ot1aQTG+/oSTmwI8t6ofaQ
bLRlugjER/fqHfyF3l+4D4OJYO0cgo/FYFBYZ6NbQdnL2uKf/Jb8rGAHzYO5sLe4
ZQOHAo+JVPAweahmoRQ4tVRDZ5ZPxnkXqk2n2U7RhffCBjspT15fpubGF0gVtcDQ
4Pj0V8wjzIZRDRF+DfMp5OaHfIlOlOI15wIDV6572hPq1Q6whrzPalmqGMbCc/PK
goasLn6T8j5BAB93ORXcbzEmPKT/I1Lw9B4qap613b489LMOx+TSX1kDj9e87YlU
6wl42oI0/BwsePTJZmJfRxZiiDY5kAmU6vQb81bZJDUwUilXnAOvWGVq0h4vFIn4
w7BhzHIgF4ldjhtIJ9w7ftLPYLDBDo3wNAMoALBTO4mGxHxI+sDczXSwfx/9UojN
WmEQU8MOhBTO/25CCW960cT2EHhuEGOwXcJNrrcNnE7nEkkLwIDatrqZdsoGBEsH
AYq87E7nCvD/Qytpjmzc7z8fVoTK924NkyyxJdq15dMAM3SO9cDDItujtA5NAt+H
YJSXZADMHFTSbhVdj/j/szngaB5k2bZov6Lt7LgET5Sflw91WFcmuXjvJ6JwJOEh
B5yyybP3jxk+vG/nBWwBjCf8awdNZLqj/VKTIGvr5T4mbmlCpmkSevuPc/2F7c9X
IUuZPg9a73ZUpXLiBVOHOEyL2mSVnQngW9tWI/01K+dAv4vjl15a3MA+QjQCpShp
5QES8I/dqqiqYcTMjmwjDOETIQ5VAw7kDpJSGSXCEtQE+nGcco3Nog==
-----END RSA PRIVATE KEY-----
igor:openssl igorcavrak$
```

zaštita <u>postojećeg</u> privatnog ključa tripleDES šifriranjem (unos passphrase-a)

podatak o načinu štićenja ključa unutar PEM zapisa

Stvaranje zaštićenog para ključeva

openssl — -bash — 102×43

```
igor:openssl igorcavrak$ openssl genrsa -aes256 -out keyB.pem 2048
Generating RSA private key, 2048 bit long modu
.......................+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for keyB.pem:
Verifying - Enter pass phrase for keyB.pem:
igor:openssl igorcavrak$ ls
keyA.pem        keyB.pem        tajno.txt
igor:openssl igorcavrak$ cat keyB.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,7A90B1A120B2B257D3EC35DF9E517C3A

1G1J7foHnhqaVAietar8rA4dJslCMXBh/oXbVIbPvKvDcJq7P+PUsjHsj3Ueew6R
9BpRiI//srbTJSIhUqyA8/eQ0NuvblRUJAevHdPWCwVJymFB3hkjGb/N5T7fUWpx
1J1JpCuJbGOtiXiNlYMEYYGDXh/cOG1XAHb01BuKIl8LaEbnTsWjvJDslEKlkKsd
JVHnHO/mcpUYskpSUXVQSgcUuLVr5hNPy/Ojc5bgTmPk9Zn0+AU9Vf4CCLsdTjsL
Z/UhX43EgqHKGgqaJSX2zPVO48dVux65Avz+VA33T3c7QLOpubJXiEX4CqCe272w
dfwzW7nNvSPSSkgdyB1SMzi2gLyEPvruzi85a9I3rpqYVx3Su/acWHJj9/di3Mi4
sozu0g1yB1N7HHkYPq7B7em2rvvInAB8wor44Z6nSK3LwcSJ0Cfrtv0qjCbB3HWC
vk5iiTPBLm4YimuTerattEQmVaJ+VPpx9NqWkNNovjYqwDOZ2F6Q19t+f02Cbtzo
GRWzp+pJJeMCUKSmiU7xbp7AlnW7agDyvezTYTpeu//HjXIOrTaOILqTuqFhhggU
5XXx/j7X6pAb9xkqKkvgCm0117ng7aFQeY0pXM9liEyxofN2uJRaLwUAGSXBnjxQ
Dzcap/GXP/+3jlG0bgLHtPc3bPC+AED+MA9U0g8CkSGFkYapJ7vCPcWvZ161Ob/1
mDyg3DzTh4Z2hHGljIfTJcrN1bsSpxtU1zz1fDrOmTOgnwuAWxomcvfrr4ppR9z7
d0zdttc7xcMWvMgfrWQ2ivclR7dlncoLF4s77MAAAHkRyw86F3du/7wtil/sn36O
9qQvJEsDy8jYGBx93H4t7W4fF3SBRdil6u6apVvgnc8aOf00gBFoSmcG6vg3vu2U
WjzL6cKDV22hDvUhaoTveJLO8zmDtXAV6K//XDNjf8QbD4rZK18knqbWJt/VjZSK
+i2bbtsbQ5fH5gSIqTvfeGpofnGi4g3XfilnrU7Jx9LDIf4d/ow1GOseWZWkwSAC
gTht4DEWitySBRJDSF56e7uHQGBABiQ9OHDbSSKiDLMnFesPQageKWWg65fysNcP
Yrs7NMtHuL3kucBpsvCRbT5UYwKeo9eqgfDjvDXzmgdJ8MR8CUREq/BdAbWvfJ2+
0MYrt2WM+JIB1wst1QNXA6WE9I50/kLc+/kKnfNS6Np/nMFvBwLFDPpQqcodVjXx
T2v+j2wI5l2n1K/dHKFfbRayYMy9muE0Kf6vO+uHeavGV82iO4J4zq+d+IvEYBhy
2KptQbd02C3m0HG6J7qH9qMWaCPx+FjPTHImrbqPneIPhWkVOzJg7YSQ4Dl+RfeQ
na6bl4tfTblv90UL1Vxf0ZmbhGEqITXq29ZDyQW2Bnb457+pXOjVxL7igcFKGdYB
pr+qxw3z33FJnzkNPNMoxRvO6p8Ho5pNr8tWvvStoKxib/u3xm8TbM4rJNSaF2/F
nVGwKjDGlcETiEXrYMkC/RKyAPGW40vvRk5IHJr+0BBp2AeaD5/tG7JXeVMl2Qfw
XqebW++n2Byb58GekquVPXQ32SaDeOFktUQQsnYaN1i3Rf1fCpGLE0ge0PrWre5Y
-----END RSA PRIVATE KEY-----
igor:openssl igorcavrak$
```

zaštita novog privatnog ključa AES-256 šifriranjem (unos passphrase-a)

Ekstrakcija javnog ključa

```
igor:openssl igorcavrak$ openssl rsa -in keyA.pem -pubout -out pubkeyA.pem
Enter pass phrase for keyA.pem:
writing RSA key
igor:openssl igorcavrak$
igor:openssl igorcavrak$ openssl rsa -in keyB.pem -pubout -out pubkeyB.pem
Enter pass phrase for keyB.pem:
writing RSA key
igor:openssl igorcavrak$ ls
keyA.pem        keyB.pem        pubkeyA.pem     pubkeyB.pem     tajno.txt
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat pubkeyA.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu98S6eSWgpSj3jbEYei8
5DJGRTWwvw3tEJxRDGW3gJXKVIjyXNCATKfX34w8GL0Q08+bnOUNza8hhDf5s0kd
jEmxumR7l73H0NveONVi1MIT3YI6XYPmIrkyYp+u8H1F+Gp7CJjBhBe+Ssr9lNcs
LwfXnU3ziWdIVFBCJoDp/FjQpOnF1Y5U6N5MrcEmfm0YkGpkB+HeCI5BPpZeV3vu
kn3G+oVz077ovl3whnc0WKzWNEE2nGzCIHHD9MMyW2Rnblyi2wHk1kj3KU30JWlO
wBxqtpSEpcz8ipSHQCLAk13HiH14i4RgbfxoCcx/qUIcqJ0H06KqYqzEN8MQwIUR
vQIDAQAB
-----END PUBLIC KEY-----
igor:openssl igorcavrak$
```

„izlazi" javni ključ (inače se podrazumijeva da se ispisuje privatni ključ)

PEM zapis javnog ključa

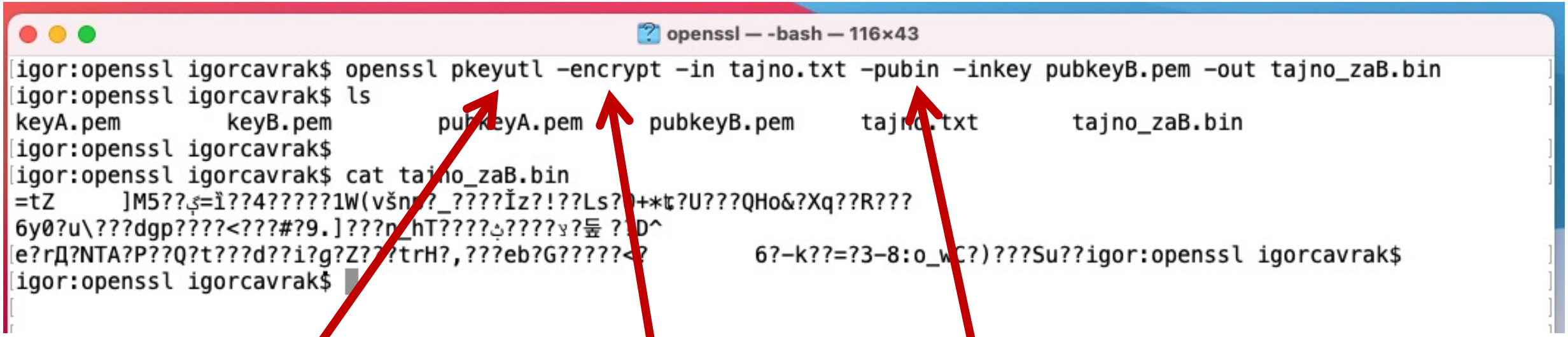
Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

Šifriranje javnim ključem primatelja

Osoba A šifrira poruku javnim ključem osobe B –
samo osoba B može dešifrirati poruku sa svojim privatnim ključem



naredba za rad s asimetričnim ključevima

operacija šifriranja

Iz pem datoteke se koristi javni ključ (inače se podrazumijeva dohvaćanje privatnog ključa)

Dešifriranje tajnim ključem primatelja

Osoba B dešifrira poruku sa svojim privatnim ključem

```
openssl — -bash — 116×43
igor:openssl igorcavrak$ ls
keyA.pem        keyB.pem        pubkeyA.pem     pubkeyB.pem     tajno.txt       tajno_zaB.bin
igor:openssl igorcavrak$ openssl pkeyutl -decrypt -in tajno_zaB.bin -inkey keyB.pem -out plain.txt
Enter pass phrase for keyB.pem:
igor:openssl igorcavrak$ ls
keyA.pem        keyB.pem        plain.txt       pubkeyA.pem     pubkeyB.pem     tajno.txt       tajno_zaB.bin
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat plain.txt
Ovo je tajna poruka koju smiju pročitati samo odabrani!

igor:openssl igorcavrak$
```

naredba za rad s asimetričnim ključevima

operacija dešifriranja

Iz pem datoteke se koristi privatni ključ

Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

Potpisivanje sažetka

Osoba A potpisuje sažetak poruke svojim privatnim ključem -
svaka osoba koja posjeduje javni ključ osobe A može provjeriti potpisani sažetak

openssl — -bash — 116×43

```
igor:openssl igorcavrak$ ls
keyA.pem        keyB.pem        plain.txt       pubkeyA.pem     pubkeyB.pem     tajno.txt       tajno_zaB.bin
igor:openssl igorcavrak$
igor:openssl igorcavrak$ openssl dgst -sha256 -sign keyA.pem -out tajno.signature tajno.txt
Enter pass phrase for keyA.pem:
igor:openssl igorcavrak$
igor:openssl igorcavrak$ cat tajno.signature
Tn:A??????????H3?n<??w?/?????c)????M??,??=N?4??{?L?9?xPg+?o?,?cVMa???<a???7u???-'?A?
                                                                                ?B?.z\??LL?d"2??4??h???J}cx???{???
r????<??!c???TJ?V.?::?¥G?O7I?v\?9~WP???r
Q???xh?(:)?'S:H???j??D?.kQ???.?$?%+?)ou"?kX???AMLX?J?tigor:openssl igorcavrak$
```

Sažetak se stvara algoritmom sha256

Sažetak se potpisuje privatnim ključem iz PEM datoteke

Rezultirajući potpis sažetka

Verifikacija potpisa

Osoba ? posjeduje javni ključ osobe A, potpisani sažetak od strane osobe A i originalnu (potpisanu) datoteku, provjerava potpis sažetka i sažetak poruke

```
openssl — -bash — 116×43
igor:openssl igorcavrak$ ls
keyA.pem        plain.txt       pubkeyB.pem     tajno.txt
keyB.pem        pubkeyA.pem     tajno.signature tajno_zaB.bin
igor:openssl igorcavrak$
igor:openssl igorcavrak$ openssl dgst -sha256 -verify pubkeyA.pem -signature tajno.signature tajno.txt
Verified OK
igor:openssl igorcavrak$
```

Sažetak je stvoren algoritmom sha256

Sažetak se verificira javnim ključem iz PEM datoteke

Datoteka s potpisanim sažetkom

Datoteka čiji se potpisani sažetak verificira

Otvoreno računarstvo

9a. OpenSSL

1. Uvod u OpenSSL
2. Sažetak poruke
3. Šifriranje simetričnim ključem
4. Stvaranje tajnog i javnog ključa
5. Šifriranje javnim ključem
6. Digitalni potpis
7. Certifikati

Zahtjev za izdavanjem certifikata (I)

```
openssl — -bash — 116×43
igor:openssl igorcavrak$ openssl req -newkey rsa:2048 -nodes -sha256 -keyout or.key -out or.csr
Generating a 2048 bit RSA private key
...........+++
..+++
writing new private key to 'or.key'
-----
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) []:HR
State or Province Name (full name) []:Croatia
Locality Name (eg, city) []:Zagreb
Organization Name (eg, company) []:FER
Organizational Unit Name (eg, section) []:ZARI
Common Name (eg, fully qualified host name) []:or.fer.uniz
Email Address []:or@fer.hr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
igor:openssl igorcavrak$
```

Korisnik stvara CSR datoteku (Certificate Signing Request) za novostvoreni par ključeva (RSA duljinke ključa od 2048 okteta) i šalje ju CA

CA svojim tajnim ključem potpisuje certifikat (uključujući korisnikov javni ključ)

Zahtjev za izdavanjem certifikata (II)

openssl — -bash — 116×43

```
igor:openssl igorcavrak$ cat or.key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDvU+zsw7JIGBnJ
Ke2/arHEJQY5QFkzDe8B8eSdhhKAb1EumA4y82OPAA9TFr8qAHoruzqHRmyF88dH
5DZSkudMNiScmfGMKH+itRAzHCwb6d2q5HqUw9u3SoQbEp6bIomiy25M3
6Wn4SuzgfWlJA683xuKF61yVJK5kExV1xYthjRVyDNOvWX281++h+muSA
y1uEMpMjF5+zX7oYEMMmN3EqydyqT9N16rI++qNbxZRL4OclvGr8/PKwF
aS6CDMWdJ6N4poTFEIzVjqtQhaoUpcSg/3yOKN5I3HK0+TbEpKKMoxyEN
x472hkiPAgMBAAECggEBAI7dmKdVww1KZcoyH1yPAoNGXsq6YQUbIjwU
kNGxr3g21o28yWkeQQt/sW59m9i473ufJK0DzHHKhAx4na5mL00tt9OX
8MxdC9fWe0iVUPsgSFHvch4eNj/ou03mgsdgRwQTJgh0lO8jJeuz6/Fp
edHTifR18qj9usRgg2UAZ9c5n9gFPi4bJN0aij+/Cflo5aHR5rpj411P
5hDomFIim4RiP6tTokzC7MPPH0JVGxNjlhcVesufbN5HoX47XOLbN7pN
cLd22eUw56bCSkrmQW5Kx9gUhEdcuGLTjD/SrQK8EuECgYEA/Wt9yTYC
/uGxF5HYZXaVMQormmwDPuNw/BNBltTMom/ZNv6BRRd67a+n76nfT2mE
2vP2M4XdEV693kczemnYYcncnYL3ApP7uSGTcZpH7AkwXuvtzENXp/eF
OXiPNBoQ8TwdGdZ0wUKGSafM+2kCgYEA8cO0cxwjml9UxkvKW4YL6wCx
ImMdZIcLXWV8jNmNV/CZPtqZKxxa3EzYMaeKLjfe+wTNn0Gt8mI90wQJ
4XOSIqgGHfzfB+dsSIrEI+YBoRBKxPlsnW36bagk2AvEL54ohHV6M9ZO
YmhLngeqfTcCgYEAt2k8uIvmTQck050JxKcDzNM5kvWoNL3voOvbzYA/
+tuIkkzQsniz96LSIJsJjCgKYy5/8TF4TC+VWOThgtjXAjD2CPriKKQ4
k5nBZM8MjsB3ybtneBalMmPqp8u2eKimtKmUu1jCOlYPmcuk5NqI5nYT
LQEI6ybjeJnKTChVoGdSNLEJQon6lQ+khkI5E0vZ7DWiSg4RdZ6neMAE
N1LfsJQdkQCpNlvCDYWP3AS4JujeSap4KhutMHqB843l/up7kMb41T9g
FmsSkS9nWUn3JZYcac0J8XBqsyMA2RgSwac88bCUtwKBgGHQiTxn0zIZ
iXovbnbII4OmXkh2pph60KCqpU5sg86hOM1v+/Rq/RVRI2gLulQlAt8h
ifzwyETzzA+SjhhJnqxeWGfyC9J969wZ778gLDntAVv2ZiHcHVbq22x6
Af6IXGZ3/7JT7JXAo7sY1f4Q
-----END PRIVATE KEY-----
igor:openssl igorcavrak$
```

openssl — -bash — 116×43

```
igor:openssl igorcavrak$ cat or.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICxzCCAa8CAQAwgYExCzAJBgNVBAYTAkhSMRAwDgYDVQQIDAdDcm9hdGlhMQ8w
DQYDVQQHDAZaYWdyZWIxDDAKBgNVBAoMA0ZFUjENMAsGA1UECwwEWkFSSTEYMBYG
A1UEAwwPb3IuZmVyLnVuaXpnLmhyMRgwFgYJKoZIhvcNAQkBFglvckBmZXIuaHIw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDvU+zsw7JIGBnJKe2/arHE
JQY5QFkzDe8B8eSdhhKAb1EumA4y82OPAA9TFr8qAHoruzqHRmyF88dH5DZSkudM
NiScmfGMKH+itRAzHCwb6d2q5HqUw9u3SoQbEp6bIomiy25M3jDBE0F86Wn4Suzg
fWlJA683xuKF61yVJK5kExV1xYthjRVyDNOvWX281++h+muSAEnJsae2y1uEMpMj
F5+zX7oYEMMmN3EqydyqT9N16rI++qNbxZRL4OclvGr8/PKwF3tUzfa0aS6CDMWd
J6N4poTFEIzVjqtQhaoUpcSg/3yOKN5I3HK0+TbEpKKMoxyENAqMtiQvx472hkiP
AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAbgCnRT4foz3twFdugZKaNYW/i00d
z5nNyK2msO8GJuQxOzcw/nonlTyLWZID/tuflt7QNd7aDZlcLPNsEj1xKjeedbV6
gPxFqPfsIKBkIHWZhgWRvzsKYW9/DdcsyMOfy9Qb0plvXhJz3HzYqdSCXYi17sQS
nlCMZBAmuCLVzIWDmBmmR7UTU6mYXBWALoMn2BWu6dzIiT5gt/tONkckcZwHsyFX
CvR5C17MSYMTUNVCEgafwQOuyvZw6gHsXLIszspESw9qACaNghqY+XFccimRxehF
QOkCeUphq9bJjFkMhxG3e2fF0SOTQQfiSSsFEwPMfSUQEPHC9wYC7pwcYA==
-----END CERTIFICATE REQUEST-----
igor:openssl igorcavrak$
```

Samo-potpisani certifikati

openssl — -bash — 116×43

```
igor:openssl igorcavrak$ openssl req -newkey rsa:2048 -nodes -sha256 -keyout or.key  -x509 -days 365 -out or.crt
Generating a 2048 bit RSA private key
.....................................................................+++
.....................+++
writing new private key to 'or.key'
-----
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) []:HR
State or Province Name (full name) []:Croatia
Locality Name (eg, city) []:Zagreb
Organization Name (eg, company) []:FER
Organizational Unit Name (eg, section) []:ZARI
Common Name (eg, fully qualified host name) []:or.fer.unizg.hr
Email Address []:or@fer.hr
igor:openssl igorcavrak$ cat or.crt
-----BEGIN CERTIFICATE-----
MIIDgDCCAmgCCQDPH7FXV6vIPjANBgkqhkiG9w0BAQsFADCBgTELMAkGA1UEBhMC
SFIxEDAOBgNVBAgMB0Nyb2F0aWExDzANBgNVBAcMBlphZ3JlYjEMMAoGA1UECgwD
RkVSMQ0wCwYDVQQLDARaQVJJMRgwFgYDVQQDDA9vci5mZXIudW5pemcuaHIxGDAW
BgkqhkiG9w0BCQEWCW9yQGZlci5ocjAeFw0yMTAxMDkyMTIzMjFaFw0yMjAxMDky
MTIzMjFaMIGBMQswCQYDVQQGEwJIUjEQMA4GA1UECAwHQ3JvYXRpYTEPMA0GA1UE
BwwGWmFncmViMQwwCgYDVQQKDANGRVIxDTALBgNVBAsMBFpBUkkxGDAWBgNVBAMM
D29yLmZlci51bml6Zy5ocjEYMBYGCSqGSIb3DQEJARYJb3JAZmVyLmhyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0K6Hp2v52SyVza/IrQ+eCXSf/hkf
+Ds4xGQZFRMsuXEPW5jSl8G8tT2b8iZoGb6+4+K8yysgOJCsqHW/I0QDqpx2TyVQ
aeRSaG3Oc1bg/zwoq/BifF9IW334jNfl8/WxR1Zm28w302uujWURI3Ni8z3IrfCc
SrkzLSd9pRUR3WlyYZKod6D9nxeQbPBjhDpIt2JMMBIrN5bs59qkqcGbMhgK7fDJ
hiXC3U79GwIULD42C8eYwlJCGHH9Ju4tcblWcOAYNr23g+41HcBW8L2CbJRudbdv
+FbSY/2jc2mvDlnD6HKOoymphUDg4yDIpsO2WzaAfJp4PCVAxfPDGHBeywIDAQAB
MA0GCSqGSIb3DQEBCwUAA4IBAQAUCRMBhHH3BKOYb2DnxdNf8y4yC1IyPlX8bD/n
y3xre3gR0BfYEnRQKZPhUn/Ak+rlwThJ8u0Dw4VKV6qJ5Exm/h2qYb5e+vQ9xnok
A/4FnQ6grQQdhHn6qkWp8dk6bk22fORxAANScP0iCOb0Cff0xTZlj5iGiZ+doQ2t
zX8LCa5hul12q4gyHBV+DixnMuJRorcKXyOKfnGe6if0Vzh3DKQXmIXW2KdQq1sb
bwZJY+BbzFb3iSdFnisJiqKa8nW8QDwAcwqvNF0FGrrAr0IDUuJmCalGDoWx3nWl
9P7a4OvbYG1g35EpN4Jk070pidiIZHf+7FhIMmiR3tZNI5a+
-----END CERTIFICATE-----
igor:openssl igorcavrak$
```

X.509 format zapisa certifikata

Period valjanosti certifikata

Samopotpisani certifikat – korisnik jamči za samog sebe da je to on ⍰

(svojim privatnim ključem potpisuje svoj javni ključ)

Pregled certifikata

openssl — -bash — 116×43

```
igor:openssl igorcavrak$ openssl x509 -text -noout -in or.crt
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 14924842678820259902 (0xcf1fb15757abc83e)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=HR, ST=Croatia, L=Zagreb, O=FER, OU=ZARI, CN=or.fer.unizg.hr/emailAddress=or@fer.hr
        Validity
            Not Before: Jan  9 21:23:21 2021 GMT
            Not After : Jan  9 21:23:21 2022 GMT
        Subject: C=HR, ST=Croatia, L=Zagreb, O=FER, OU=ZARI, CN=or.fer.unizg.hr/emailAddress=or@fer.hr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d0:ae:87:a7:6b:f9:d9:2c:95:cd:af:c8:ad:0f:
                    9e:09:74:9f:fe:19:1f:f8:3b:38:c4:64:19:15:13:
                    2c:b9:71:0f:5b:98:d2:97:c1:bc:b5:3d:9b:f2:26:
                    68:19:be:be:e3:e2:bc:cb:2b:20:38:90:ac:a8:75:
                    bf:23:44:03:aa:9c:76:4f:25:50:69:e4:52:68:6d:
                    ce:73:56:e0:ff:3c:28:ab:f0:62:7c:5f:48:5b:7d:
```

Verifikacija certifikata

```
openssl — -bash — 116×43
igor:openssl igorcavrak$ openssl verify -verbose -CAfile or.crt or.crt
or.crt: OK
igor:openssl igorcavrak$
```

Certifikat CA koja je potpisala verificirani certifikat

Certifikat koji se verificira

U ovom slučaju verificiramo samopotpisani certifikat