

Sigurnost u Internetu

Laboratorijske vježbe

Vježba 1

Kriptografske operacije

Jakov Dorontić, 0036503608

1) Provjera digitalnog potpisa i dešifriranje podataka

Pomoću alata *GNU Privacy Guard* (GnuPG) uvezujemo javni ključ u GnuPG bazu pozivom naredbe:

```
gpg --import key.gpg
```

Nakon što je ključ uvezen u GnuPG bazu, provjeravamo (verificiramo) ispravnost digitalnog potpisa za datoteku `secret.bin` pozivom naredbe:

```
gpg --verify secret.bin
```

Izvršavanjem navedene naredbe dobivamo informaciju o tome kada je ključ stvoren (21. listopada 2015) i je li datoteka uistinu bila potpisana tim javnim ključem (Good signature from "Internet Security ..."). Kako bi dešifrirali sadržaj šifrirane datoteke moramo pozvati naredbu:

```
gpg --decrypt secret.bin
```

Dekriptirani sadržaj `secret.bin` datoteke je:

```
KOREAN apple XBOX jack nut ROPE EGG ZIP QUEEN jack queen BESTBUY  
USA MUSIC USA 3 SKYPE nut usa WALMART walmart ZIP 6 EGG 3 5 jack  
yelp DRIP EGG ZIP yelp 9 LAPTOP egg 7 7 YELP coffee apple
```

Ukoliko iz gore navedenog ispisa uzmemo samo prvo slovo svake riječi, dobivamo simetričan ključ koji zapišemo u novu datoteku:

```
KaXjnREZQjqBUMU3SnuWwZ6E35jyDEZy9Le77Yca
```

`symmetric_key.txt`

Sada dekriptiramo datoteku `data.bin` pozivom naredbe:

```
gpg --batch --yes --passphrase-file  
symmetric_key.txt --decrypt data.bin >  
data_decrypted.bin
```

Nakon par sekundi datoteka `data_decrypted.bin` je stvorena. Kako bi saznali o kojem je tipu datoteke riječ pozivamo naredbu: `file *` i saznajemo da je riječ o videozapisu (ISO Media, MP4 v2).

Dodatno, ukoliko pozovemo naredbu:

```
sha256sum data_decrypted.bin
```

Dobivamo SHA256 sažetak pomoću kojeg se uvjeravamo da smo točno dekriptirali sadržaj datoteke `data.bin`:

```
3059724a4a32088244560552b09bb425db76f71c6143ed0af20ae62b7861ea96
```

2) Pregledavanje dešifriranih podataka

Dešifrirana datoteka je video predavanje koje je održao Mikko Hyppönen na TED Talks konferenciji. Predavanje je vezano za temu sigurnosti na Internetu i približno traje 17 minuta.



3) Digitalno potpisivanje

Za potpisivanje datoteke s vlastitim digitalnim potpisom potrebno je kreirati vlastiti privatni ključ sljedećom naredbom:

```
gpg --gen-key
```

Navedena naredba će dodatno zatražiti ime korisnika, email adresu i passphrase. Sada na raspolaganju imamo vlastiti privatni RSA ključ i pripadni javni RSA ključ (koji su nam na raspolaganju sljedeće dvije godine, tj. do 11.10.2022).

Datoteku koji želimo potpisati je `student_info.txt` koja sadrži ime, prezime i JMBAG. Datoteka se potpisuje sljedećom naredbom:

```
gpg --output student_info.bin --sign
student_info.txt
```

Naredba stvara novu (potpisanu) datoteku `student_info.bin`.

Kako bi ostali korisnici na Internetu mogli provjeriti da je datoteka potpisana ranije stvorenim privatnim ključem, potrebno je izvesti pripadni javni ključ naredbom:

```
gpg --armor --export jakov.dorontic@fer.hr >
jakov_public_key.gpg
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBF+DOsUBDAD+awppsJFVrVLb8q//O5LdF3aRkx1+7rnfmZ3fpmRtq9LyPjyo
ZSwuFg83a/Nqbim69Gwtvonhq4MSPOZEf4vc5rlrRqoVkyzVE1fhfH6t9/oH/7VL
...
7UA9/xdEEfbBLsQQeqErYlXfuqpKyLsxskefM01A
=em3A
-----END PGP PUBLIC KEY BLOCK-----
```

`jakov_public_key.gpg`

4) Šifriranje tajnih podataka

Datoteka `top_secret.txt` koja sadrži tajne podatke i koju želimo šifrirati javnim RSA ključem (čiji je vlasnik `sui@fer.hr`) se šifrira pozivom naredbe:

```
gpg --output top_secret.bin --encrypt --recipient
sui@fer.hr top_secret.txt
```

Naredba stvara šifriranu datoteku `top_secret.bin`.

5) Brzina simetričnih i asimetričnih algoritama

Simetrični algoritam	Brzina šifriranja	Brzina dešifriranja	Komentar
AES-256-ECB	1.028s	3.199s	Najbrži, nesiguran
AES-256-CBC	2.659s	2.199s	
AES-256-CTR	2.379s	2.196s	Najsigurniji
DES-EDE3	5.723s	7.184s	Najsporiji
DES-EDE3-CBC	5.728s	6.736s	

Tablica 5.1: Brzine šifriranja i dešifriranja simetričnih algoritama

Asimetrični algoritam	Broj blokova potpisanih u 10s	Broj blokova provjerenih u 10s	Omjer brzina
RSA-512	86305 bita	1387296 bita	16.07 puta brža provjera
RSA-3072	1150 bita	57588 bita	50.08 puta brža provjera
ECDSA-160	17727 bita	23562 bita	1.33 puta brža provjera
ECDSA-521	7927 bita	3941 bita	2.01 puta brže potpisivanje

Tablica 5.2: Brzine potpisivanja i provjere potpisa asimetričnih algoritama

6) SSH

Za spajanje na udaljeni poslužitelj *mrepro.tel.fer.hr* putem protokola SSH (eng. *Secure Shell*) potrebno je pozvati slijedeću naredbu:

```
ssh jd50360@mrepro.tel.fer.hr
```

Za preuzimanje datoteke *sui.db* s poslužitelja potrebno je pozvati naredbu:

```
scp jd50360@mrepro.tel.fer.hr:sui.db ~/
```

Promet prilikom prijave na udaljeni poslužitelj snimljen je Wireshark alatom (*Slika 6.1*). Može se vidjeti da je vjerodajnica kriptirana ključem generiranim Diffie-Hellman algoritmom koji je jako ranjiv na man-in-the-middle napad. Kako bi se bolje zaštitili potrebno je generirati par ključeva koji će se koristiti za spajanje na udaljeni poslužitelj pozivom naredbe:

```
ssh-keygen
```

Kreirani javni ključ potrebno je kopirati na poslužitelj *mrepro.tel.fer.hr* pozivom naredbe:

```
ssh-copy-id jd50360@mrepro.tel.fer.hr
```

Capturing from Wireless Network Connection 4 (host 161.53.19.47)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.5	161.53.19.47	TCP	66	49262 → 22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.009282	161.53.19.47	192.168.100.5	TCP	66	22 → 49262 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM=1 WS=64
3	0.009462	192.168.100.5	161.53.19.47	TCP	54	49262 → 22 [ACK] Seq=1 Ack=1 Win=66364 Len=0
4	0.017702	192.168.100.5	161.53.19.47	SSHv2	95	Client: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3)
5	0.021348	161.53.19.47	192.168.100.5	SSHv2	93	Server: Protocol (SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u3)
6	0.022683	192.168.100.5	161.53.19.47	SSHv2	1414	Client: Key Exchange Init
7	0.027246	161.53.19.47	192.168.100.5	SSHv2	1102	Server: Key Exchange Init
8	0.030370	161.53.19.47	192.168.100.5	TCP	54	22 → 49262 [ACK] Seq=1 Ack=42 Win=29248 Len=0
9	0.030454	192.168.100.5	161.53.19.47	TCP	54	49262 → 22 [ACK] Seq=1402 Ack=1088 Win=65276 Len=0
10	0.043664	192.168.100.5	161.53.19.47	SSHv2	102	Client: Diffie-Hellman Key Exchange Init
11	0.058961	161.53.19.47	192.168.100.5	SSHv2	826	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=140)
12	0.070233	192.168.100.5	161.53.19.47	SSHv2	70	Client: New Keys
13	0.070921	192.168.100.5	161.53.19.47	SSHv2	98	Client: Encrypted packet (len=44)
14	0.074323	161.53.19.47	192.168.100.5	SSHv2	98	Server: Encrypted packet (len=44)
15	0.074875	192.168.100.5	161.53.19.47	SSHv2	122	Client: Encrypted packet (len=68)
16	0.079757	161.53.19.47	192.168.100.5	SSHv2	130	Server: Encrypted packet (len=76)
17	0.080381	192.168.100.5	161.53.19.47	SSHv2	146	Client: Encrypted packet (len=92)
18	0.081811	161.53.19.47	192.168.100.5	TCP	60	22 → 49262 [ACK] Seq=1860 Ack=1510 Win=31936 Len=0
19	0.081893	192.168.100.5	161.53.19.47	TCP	54	[TCP Dup ACK 17#1] 49262 → 22 [ACK] Seq=1670 Ack=1980 Win=66244 Len=0
20	0.084073	161.53.19.47	192.168.100.5	SSHv2	130	Server: Encrypted packet (len=76)
21	0.281214	192.168.100.5	161.53.19.47	TCP	54	49262 → 22 [ACK] Seq=1670 Ack=2056 Win=66168 Len=0
22	8.798466	192.168.100.5	161.53.19.47	SSHv2	202	Client: Encrypted packet (len=148)
23	8.807004	161.53.19.47	192.168.100.5	SSHv2	82	Server: Encrypted packet (len=28)
24	8.807729	192.168.100.5	161.53.19.47	SSHv2	166	Client: Encrypted packet (len=112)
25	8.811236	161.53.19.47	192.168.100.5	SSHv2	834	Server: Encrypted packet (len=780)
26	9.008020	192.168.100.5	161.53.19.47	TCP	54	49262 → 22 [ACK] Seq=1930 Ack=2864 Win=65360 Len=0
27	9.011024	161.53.19.47	192.168.100.5	SSHv2	98	Server: Encrypted packet (len=44)
28	9.011907	192.168.100.5	161.53.19.47	SSHv2	1150	Client: Encrypted packet (len=1096)
29	9.016622	161.53.19.47	192.168.100.5	SSHv2	162	Server: Encrypted packet (len=108)
30	9.017599	161.53.19.47	192.168.100.5	SSHv2	146	Server: Encrypted packet (len=92)
31	9.017628	161.53.19.47	192.168.100.5	SSHv2	90	Server: Encrypted packet (len=36)
32	9.017732	192.168.100.5	161.53.19.47	TCP	54	49262 → 22 [ACK] Seq=3026 Ack=3144 Win=65080 Len=0
33	9.049479	161.53.19.47	192.168.100.5	SSHv2	106	Server: Encrypted packet (len=52)
34	9.248045	192.168.100.5	161.53.19.47	TCP	54	49262 → 22 [ACK] Seq=3026 Ack=3196 Win=65028 Len=0

Frame 6: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface \Device\NPF_{1CE7E899-98D1-4392-B549-50B1CFE8E6F1}, id 0

Ethernet II, Src: KingjonD_2b:07:05 (00:13:ef:2b:07:05), Dst: HuaweiTe_9a:93:6f (48:f8:db:9a:93:6f)

Internet Protocol Version 4, Src: 192.168.100.5, Dst: 161.53.19.47

Transmission Control Protocol, Src Port: 49262, Dst Port: 22, Seq: 42, Ack: 40, Len: 1360

SSH Protocol

0000 48 f8 db 9a 93 6f 00 13 ef 2b 07 05 08 00 45 00 H...o...+...E

0010 05 78 6a bf 40 00 00 06 b1 ae c0 a8 64 05 a1 35 .xj@...d..5

0020 13 2f c0 6e 00 16 c9 cd 1f 99 0c f3 21 bd 50 18 ./-n...:..P

0030 40 c5 a4 f0 00 00 00 00 05 4c 05 14 38 d6 4d 0e @.....L..8.M

0040 5f 5b b5 24 58 98 d6 0d 19 2d c8 7c 00 00 01 30 [_.\$X...-|...0

0050 63 75 72 76 65 32 35 35 31 39 2d 73 68 61 32 35 curve25519-sha25

0060 36 2c 63 75 72 76 65 32 35 35 31 39 2d 73 68 61 6,curve2 5519-sha

0070 32 35 36 40 6c 69 62 73 73 68 2e 6f 72 67 2c 65 256@libs sh.org,e

0080 63 64 68 2d 73 68 61 32 2d 6e 69 73 74 70 32 35 cdh-sha2 -nistp25

0090 36 2c 65 63 64 68 2d 73 68 61 32 2d 6e 69 73 74 6,ecdh-s ha2-nist

00a0 70 33 38 34 2c 65 63 64 68 2d 73 68 61 32 2d 6e p384,ecd h-sha2-n

00b0 69 73 74 70 35 32 31 2c 64 69 66 66 69 65 2d 68 istp521, diffie-h

00c0 65 6c 6c 6d 61 6e 2d 67 72 6f 75 70 2d 65 78 63 ellman-g roup-exc

Transmission Control Protocol (tcp), 20 byte(s) | Packets: 34 · Displayed: 34 (100.0%) | Profile: Default

Slika 6.1:Promet prilikom spajanja na udaljeni poslužitelj