SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

2020

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.bit` 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 slijedećom 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/xdEEfbBLsQQeqErY1XfuqpKyLsxskefMO1A
=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:

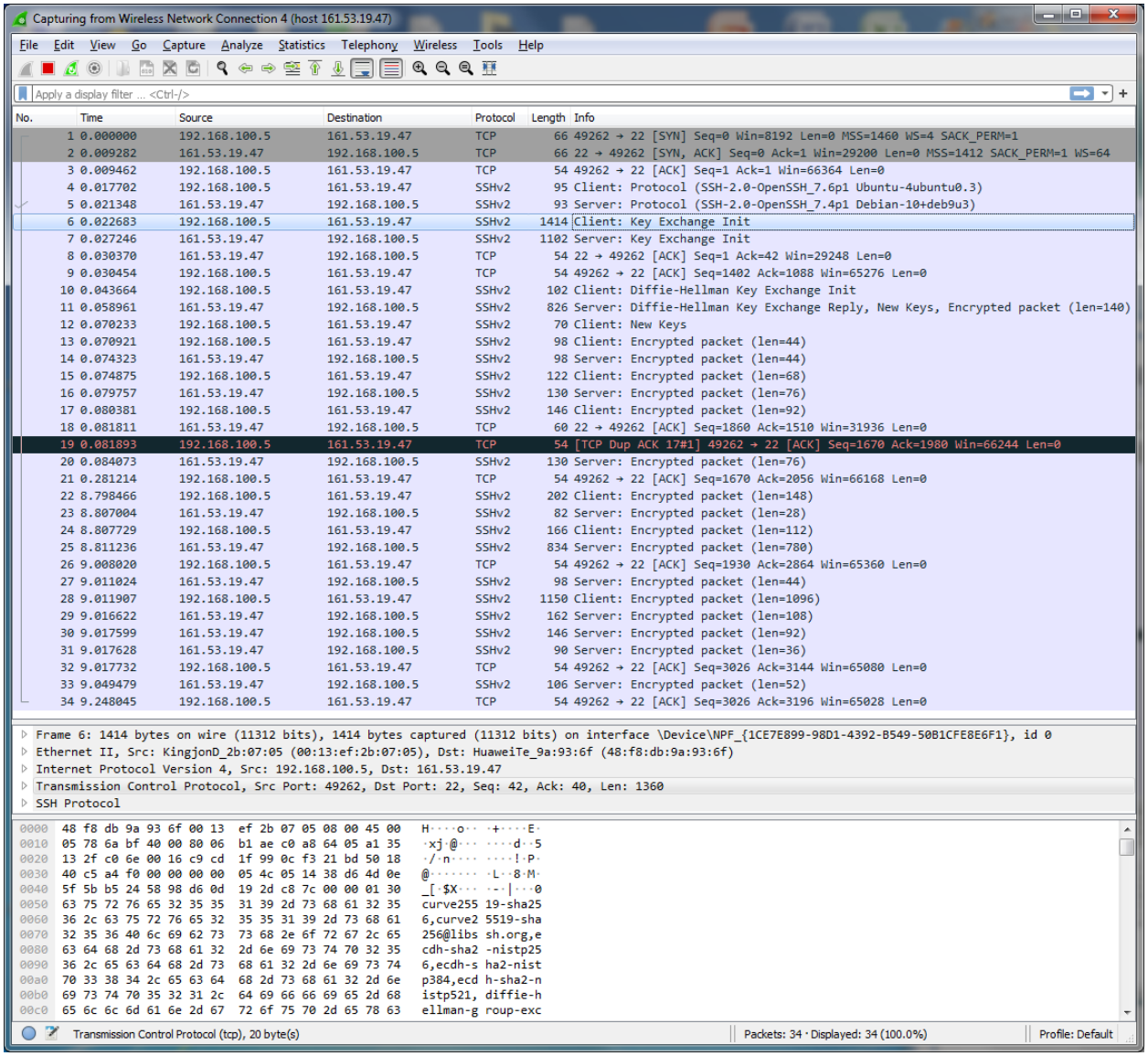
```
scp jd50360@mrepro.tel.fer.hr:sui.db ~/
```

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
```



Slika 6.1:Promet prilikom spajanja na udaljeni poslužitelj