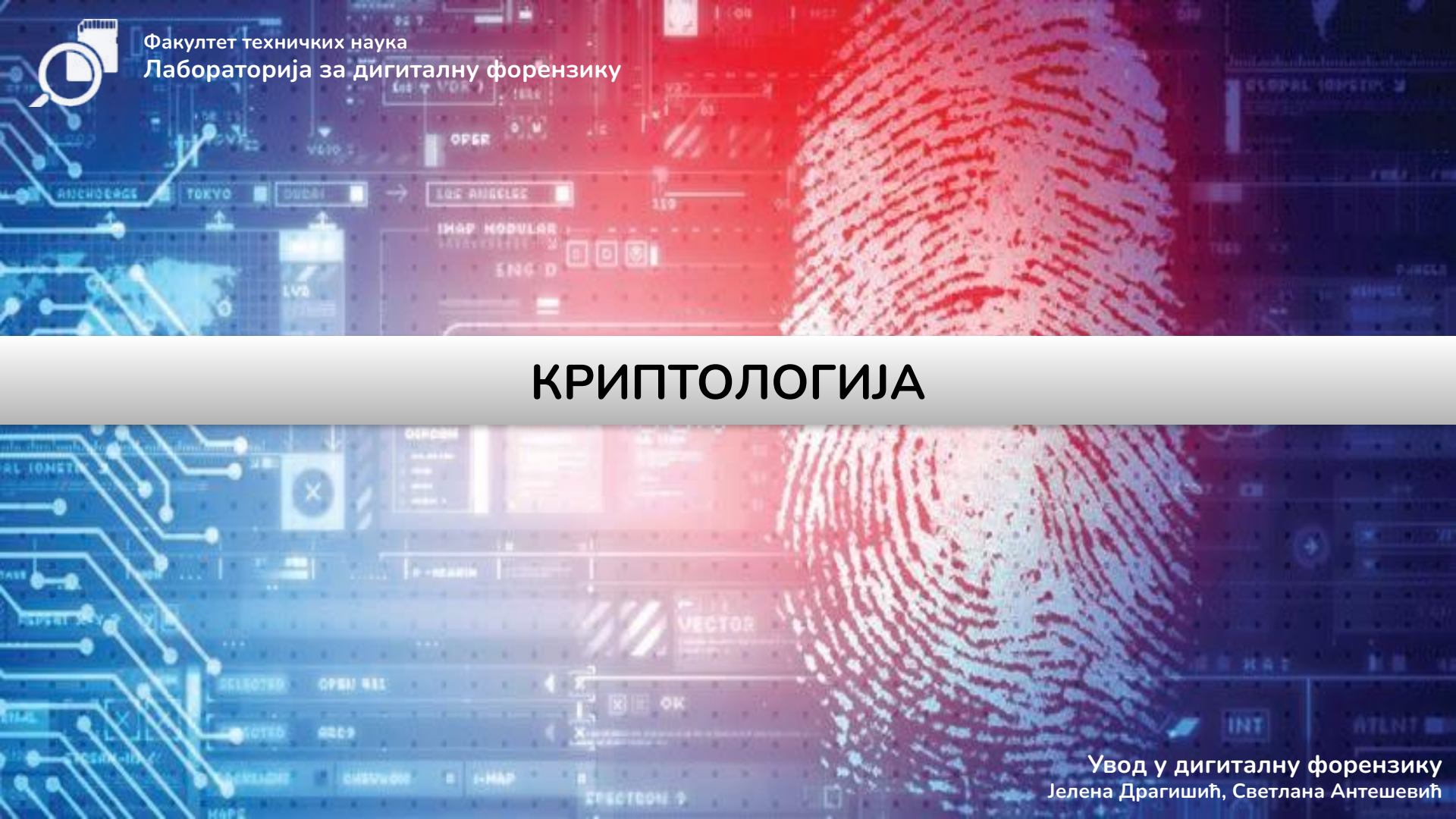


Факултет техничких наука
Лабораторија за дигиталну форензику

КРИПТОЛОГИЈА

Увод у дигиталну форензику
Јелена Драгишић, Светлана Антешевић

КРИПТОЛОГИЈА

- ➔ Криптологија је наука која се бави техникама заштите и напада на тајност (поверљивост) и интегритет порука.
- ➔ Дели се на **криптографију** и **криптоанализу**.

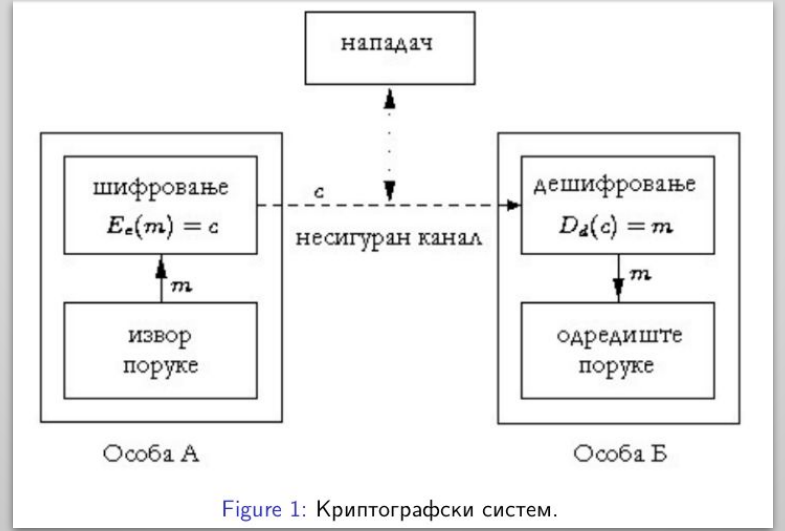


Figure 1: Криптографски систем.

КРИПТОЛОГИЈА

Шифровање (енг. encryption) је поступак трансформисања отворене поруке у шифрат.

Дешифровање (енг. decryption) је поступак трансформисања шифрата у отворени текст (уз познавање кључа).

Декрипција је поступак трансформације шифрата у отворени текст (без познавања кључа). Претпоставља се да су познати (бар) функција шифровања, функција дешифровања и да је потребно пронаћи само кључ.

Кључ је параметар који параметризује функције шифровања и дешифровања.

КРИПТОГРАФИЈА

КРИПТОГРАФИЈА

Криптографија је грана криптологије која се бави техникама заштите тајности (поверљивости) и интегритета порука.

Криптографске системе можемо поделити:

- Симетричне
  - Проточни криптографски системи (енг. Stream ciphers) - OTP, RC4, A5/2
  - Блок криптографски систем (енг. Block ciphers) - Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish
- Асиметричне - Diffie-Hellman, Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC)
- Хибридне

КРИПТОГРАФИЈА

Шифровање и дешифровање датотеке

ccrypt - Алат командне линије који се користи за шифровање и дешифровање датотека на unix оперативним системима. Заснован је на AES криптографском систему.

Шифровање датотеке:

$ ccrypt naziv_datoteke.txt

Дешифровање датотеке:

$ ccrypt -d naziv_datoteke.txt.cpt
Enter decryption key:

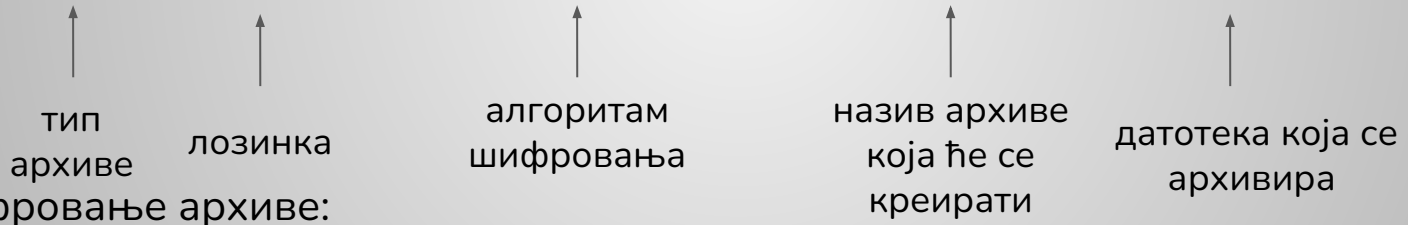
КРИПТОГРАФИЈА

Шифровање и дешифровање архиве

7za - Алат који подржава неколико различитих алгоритама за компресију и шифровање. Шифровање засновано на AES-256 криптографском систему.

Шифровање архиве:

$ 7za a -tzip -p<lozinka> -mem=AES256 sifrovana_arhiva.zip datoteka.pdf



Дешифровање архиве:

$ 7za e sifrovana_arhiva.zip

Enter password (will not be echoed):

КРИПТОГРАФИЈА

Шифровање и дешифровање система датотека

cryptsetup - алат командне линије за unix ос који нуди могућност шифровања и дешифровања партиција. Има интегрисану подршку за Linux Unified Key Setup (LUKS) - је спецификација за шифровање блок уређаја на Linux-у.

$ sudo fdisk -l <- Преглед партиција
$ sudo cryptsetup luksFormat /dev/sdb <- Форматирање и шифровање партиције као LUKS
$ sudo cryptsetup luksOpen /dev/sdb sdb1 <- Дешифровање и креирање логичке партиције /dev/mapper/sda1
$ sudo mkfs.ext4 /dev/mapper/sda1 <- Форматирање логичке партиције
$ sudo mount /dev/mapper/sda1 direktorijum <- Маунтовање логичке партиције /dev/mapper/sda1 у директоријум
$ sudo umount direktorijum <-Анмаунтовање логичке партиције
$ sudo cryptsetup luksClose /dev/sda1 <- Затварање дешифроване партиције LUKS

КРИПТОГРАФИЈА

Шифровање мрежног саобраћаја

TLS (Transport Layer Security) protocol - обезбеђује безбедносне принципе као што су аутентификација страна које комуницирају, аутентификација порука, поузданост и интегритет порука које се размењују.

Безбедносни механизми протокола TLS заснивају се на криптографским техникама, те се за аутентификацију порука и шифровање размењених података користи криптографија тајног кључа, а за аутентификацију страна које комуницирају – криптографија јавног кључа.

КРИПТОГРАФИЈА

Дешифровање мрежног саобраћаја

1. Креирати датотеку **sslkeylog.log** у оквиру **/home/kali** директоријума. Сви кључеви који се размене између веб-претраживача (клијента) и сервера током TLS протокола смештају се у датотеку sslkeylog.log.
2. У оквиру једне сесије емулатора терминала извести варијаблу **SSLKEYLOGFILE** и покренути веб претраживач.

   $ export SSLKEYLOGFILE=~/sslkeylog.log

   $ chromium

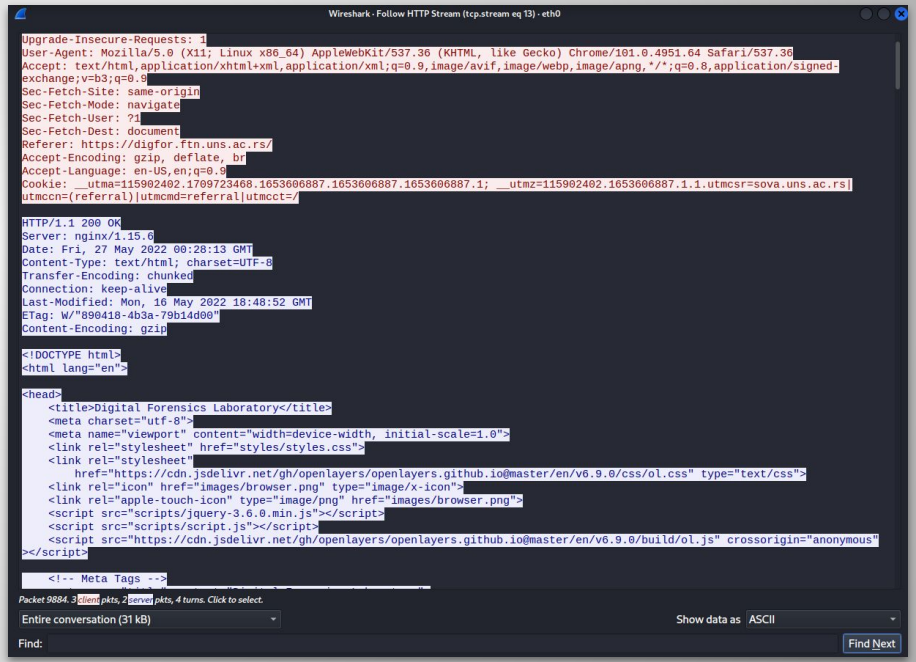
3. Покренути алат **Wireshark** и започети снимање
4. Погодити веб-сајт из веб претраживача (нпр. digfor.ftn.uns.ac.rs)
5. Након завршетка снимања мрежног саобраћаја, у алату Wireshark поставити путању до лога са кључевима на путању до датотеке sslkeylog.log. (опција Edit/Preferences/Protocols/TLS/ Pre-Master-Secret log filename).

КРИПТОГРАФИЈА

Дешифровање мрежног саобраћаја

Резултат су дешифровани токови мрежног саобраћаја чији је увид могућ кроз опцију **Follow / HTTP Stream** у Wireshark алату.

Могуће је сачувати HTTP stream као http датотеку и отворити страницу у претраживачу.



КРИПТОГРАФИЈА

Криптографске хеш функције

Хеш функције или сажимајуће функције (енг. Hash functions) су функције које пресликавају улаз променљиве дужине на излаз фиксне дужине.

Криптографске хеш функције су хеш функције које имају следеће особине: (1) једносмерне су и (2) промена једног бита у улазу мења у просеку пола битова у излазу.

Користе се као градивни елементи: система дигиталних потписа, система аутентификације порука итд.

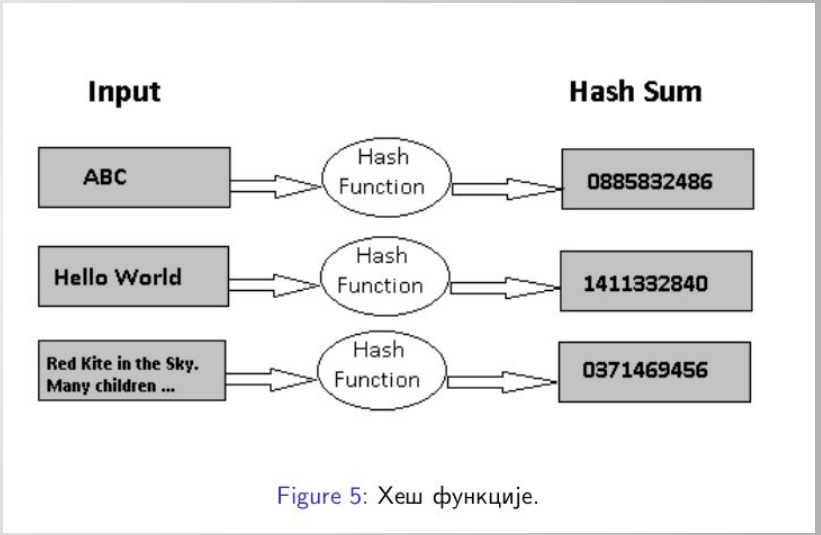


Figure 5: Хеш функције.

КРИПТОГРАФИЈА

Криптографске хеш функције

Примери: Message Digest 5 (MD5), Secure Hashing Algorithm (SHA)

```
$ md5sum datoteka.pdf
a89c481d040ba9158a735e847e1fc93d  datoteka.pdf

$ sha1sum datoteka.pdf
9b88e10acca2ec3a85d53d239af69911b8885c85  datoteka.pdf

$ sha256sum datoteka.pdf
929ad62f346177b306f6b26c7e01001cf9eb6bde7361c8aa5cf53a6067a2a688  datoteka.pdf

$ sha512sum datoteka.pdf
f75e2a5b4b8379a39c3fd850ba9c3f3afc21affb75055d54c78ec7de0dd71c6bfa6f8b99f3670ff
c77dc45f8d9ed3f416a5c297de8f6d7600d3e097f34254976  datoteka.pd
```

Факултет техничких наука
Лабораторија за дигиталну форензику

КРИПТОАНАЛИЗА

КРИПТОАНАЛИЗА

Криптоанализа је грана криптологије која се бави техникама напада на тајност (поверљивост) и интегритет порука.

Ако две стране желе да тајно комуницирају, једино што држе у тајности је кључ(еви) који користе.

Није пожељно заснивати сигурност криптографског система на тајности функција шифровања и дешифровања (историја је показала да је ово веома тешко!)

КРИПТОАНАЛИЗА

Декриптовање датотеке

ccguess - Алат командне линије који се користи за проналажење кључа за дешифровање датотеке, која је шифрована помоћу ccrypt алата.

$ ccguess datoteka.pdf.cpt

КРИПТОАНАЛИЗА

Декриптовање архиве

zip2john - Алат командне линије који се користи за проналажење хешираних вредности у садржају архиве, које ће бити крековане:

$ sudo zip2john sifrovana_arhiva.zip > hash_to_crack.txt ← датотека у коју се смештају хеширане вредности

john - Алат командне линије за крековање лозинке помоћу речника потенцијалних лозинки. Kali Linux доноси речник **rockyou.txt** смештен на локацији /usr/share/wordlists.

$ sudo john --format=zip hash_to_crack.txt --wordlist=rockyou.txt

```
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 626424 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
PASS                    (sifrovana_arhiva.zip/datoteka.pdf)
Session completed
```

КРИПТОАНАЛИЗА

Декриптовање система датотека

bruteforce-luks - Алат командне линије који омогућава крековање система LUKS верзије 1 и 2.

Потребно је проверити верзију система за шифровање LUKS:

$ sudo cryptsetup luksDump /dev/sdb1 ← Назив партиције која је шифрована

```
LUKS header information
Version:        2
Epoch:          3
Metadata area:  16384 [bytes]
Keyslots area:  16744448 [bytes]
UUID:           ec528d20-5627-49ce-9d5b-e568363b6fd8
...
```

КРИПТОАНАЛИЗА

Декриптовање система датотека

Декриптовање партиције помоћу параметара:

$ sudo bruteforce-luks -t 2 -l 4 -m 4 -b “PA” -e “S” -v 1 /dev/sdb

Tried / Total passwords: 28 / 62
Tried passwords per second: 0.297972
Last tried password: PATS
Total space searched: 45.161290%
ETA: Thu 26 May 2022 05:08:32 PM CDT
Password found: PASS

- ➔ -t број нити
- ➔ -l минималан број карактера
- ➔ -m максималан број карактера
- ➔ -b низ карактера којима лозинка започиње
- ➔ -e низ карактера којима лозинка завршава
- ➔ -v исписивање лога на задат број секунди

КРИПТОАНАЛИЗА

Декриптовање система датотека

Декриптовање шифроване слике партиције помоћу речника rockyou.txt:

$ sudo bruteforce-luks -t 2 -v 1 -f rockyou.txt slika.img

- ➔ -t број нити
- ➔ -v исписивање лога на задат број секунди
- ➔ -f путања до речника

Коришћени алати

- ccrypt
- 7za
- cryptsetup
- md5sum, sha1sum, sha256sum, sha512sum
- ccguess
- zip2john
- john
- bruteforce-luks