ASPIRA®
UNIVERSITY COLLEGE

KOLEGIJ

Sigurnost informacijskih sustava

Laboratorijska vježba br.1

Teme:

- Kriptografija
- Simetrična kriptografija
- Asimetrična kriptografija

U ovom kolegiju ćemo detaljnije obrađivati razne teme iz sigurnosti informacijskih sustava.

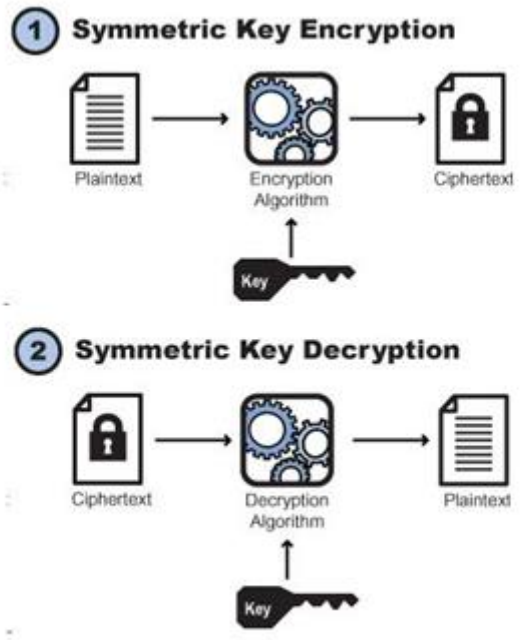
Tijekom kolegija ćemo raditi s Cryptool alatom, Kali Linux distribucijom, Pythonom, itd…

Prva laboratorijska vježbe se odnosi na opće teme iz kriptografije, uključujući simetričnu i asimetričnu kriptografiju.

Tijekom vježbe ćemo proći osnove simetrične i asimetrične kriptografije. Za testiranje ćemo koristiti Cryptool (https://www.cryptool.org/en/), tj. CT1 ediciju, alat za

demonstriranje i objašnjavanje kriptografskih funkcija i mehanizama.

Simetrična kriptografija



Zadatak počinjemo s jednom klasičnom kriptografskom metodom kao što je Caesar. Nastaviti ćemo s kriptoanalizom jednostavne supstitucijske šifre.

Što je simetrična kriptografija?

Kriptografija simetričnih ključeva (ili simetrično šifriranje) vrsta je sheme šifriranja u kojoj se isti ključ koristi i za šifriranje i dešifriranje poruka. Takva metoda kodiranja podataka uvelike se koristila proteklih desetljeća kako bi se olakšala tajna komunikacija između vlada i vojnika. U današnje vrijeme simetrični ključni algoritmi naširoko se primjenjuju u raznim vrstama računalnih sustava radi poboljšanja sigurnosti podataka.

Na koji način radi?

Sheme simetričnog šifriranja oslanjaju se na jedan ključ koji se dijeli između dva ili više korisnika. Isti se ključ koristi za šifriranje i dešifriranje takozvanog otvorenog teksta (koji predstavlja poruku ili dio podataka koji se kodira), iliti eng. **plaintext**. Postupak šifriranja sastoji se od pokretanja otvorenog teksta (ulaza) kroz algoritam šifriranja nazvan šifra, koji zauzvrat generira šifrični tekst (izlaz).

Ako je shema šifriranja dovoljno jaka, jedini način na koji osoba može pročitati ili pristupiti informacijama sadržanima u šifriranom tekstu je pomoću odgovarajućeg ključa za dešifriranje. Proces dešifriranja je u osnovi pretvaranje šifričnog teksta u otvoreni tekst.

Sigurnost simetričnih sustava šifriranja temelji se na tome koliko je teško nasumično pogoditi odgovarajući ključ da bi ih se probilo. Na primjer, 128-bitni ključ trebao bi tražiti milijarde godina da se koristi uobičajenim računalnim hardverom. Što je ključ za šifriranje duži, to ga je teže probiti. Ključevi duljine 256 bita općenito se smatraju vrlo sigurnim i teoretski otpornim na kvantne računalne napade.

Dvije najčešće simetrične sheme šifriranja koje se danas koriste temelje se na blok i tok šiframa. Blok šifre grupiraju podatke u blokove unaprijed određene veličine, a svaki se blok šifrira pomoću odgovarajućeg algoritma ključa i enkripcije (npr., 128-bitni otvoreni tekst šifriran je u 128-bitni šifrotekst). S druge strane, šifre toka ne šifriraju podatke otvorenog teksta blokovima, već 1-bitnim koracima (1-bitni otvoreni tekst se istovremeno šifrira u 1-bitni šifrotekst).

Simetrično vs. asimetrično kriptiranje

Simetrična enkripcija jedna je od dvije glavne metode šifriranja podataka u modernim računalnim sustavima. Drugi je asimetrična enkripcija, što je glavna primjena kriptografije javnog ključa. Glavna razlika između ovih metoda je činjenica da asimetrični sustavi koriste dva ključa, a ne onaj koji se koristi u simetričnim shemama. Jedan od ključeva može se javno dijeliti (javni ključ), dok se drugi mora držati u privatnom (privatni ključ).

Upotreba dvije šifre umjesto jedne također stvara razne funkcionalne razlike između simetrične i asimetrične enkripcije. Asimetrični algoritmi su složeniji i sporiji od simetričnih. Budući da su javni i privatni ključevi koji se koriste u asimetričnoj enkripciji u određenoj mjeri matematički povezani, sami ključevi moraju biti znatno duži kako bi pružili sličnu razinu sigurnosti koju nude kraći simetrični ključevi.

Moderna upotreba

Algoritmi simetrične enkripcije upotrijebljeni su u mnogim modernim računalnim sustavima kako bi se poboljšala sigurnost podataka i privatnost korisnika. Napredni standard šifriranja (AES) koji se široko koristi u aplikacijama za sigurnu razmjenu poruka i pohrani u oblaku jedan je istaknuti primjer simetrične šifre.

Osim implementacije softvera, AES se također može izravno implementirati u računalni hardver. Simetrične sheme enkripcije zasnovane na hardveru obično koriste AES 256, što je specifična varijanta Naprednog standarda šifriranja koji ima ključnu veličinu od 256 bita.

Prednosti i nedostaci

Simetrični algoritmi pružaju prilično visoku razinu sigurnosti, a istovremeno omogućuju da se poruke brzo šifriraju. Relativna jednostavnost simetričnih sustava također je logistička prednost, jer oni zahtijevaju manje računalne snage od asimetričnih. Osim toga, sigurnost koja se pruža simetričnim šifriranjem može se povećati jednostavno povećanjem duljine ključa. Za svaki pojedinačni bit dodan u duljinu simetričnog ključa, poteškoća probijanja šifriranja napadom grube sile eksponencijalno se povećava.

Iako simetrično šifriranje nudi širok spektar prednosti, uz njega je povezan jedan glavni nedostatak: inherentni problem prijenosa ključeva koji se koriste za šifriranje i dešifriranje podataka. Kad se ovi ključevi dijele preko nezaštićene veze, ranjivi su da ih presretnu zlonamjerne treće strane. Ako neovlašteni korisnik dobije pristup određenom simetričnom ključu, sigurnost svih podataka šifriranih pomoću tog ključa je ugrožena. Da bi riješili taj problem, mnogi web protokoli koriste kombinaciju simetrične i asimetrične enkripcije za uspostavljanje sigurnih veza. Među najistaknutijim primjerima takvog

hibridnog sustava je kriptografski protokol Transport Layer Security (TLS) koji se koristi za osiguranje velikih dijelova modernog interneta.

Također treba napomenuti da su sve vrste računalnih enkripcija podložne ranjivostima zbog nepravilne implementacije. Iako dovoljno dugačak ključ može činiti grubi napad (eng. Brute force attack) matematički nemogućim, pogreške u implementaciji koje programeri čine često stvaraju slabosti koje otvaraju put za napade.

ZADACI

U ovoj ćemo vježbi pokazati i proučiti predstavnika klasičnih šifri, Cezarovu šifru. Napraviti ćemo i kriptoanalizu jednostavne permutacijske šifre.

Cezarova šifra spada u kategoriju monoalfabetskih zamjenskih šifra (tj. svaki će element iz otvorenog teksta biti zamijenjen jedinstvenim elementom iz prostora šifriranog teksta). Iz tog razloga, šifrirani tekst zadržava relativnu frekvenciju na kojem se elementi čistog teksta pojavljuju u odgovarajućem otvorenom tekstu.

Više informacija:

- https://en.wikipedia.org/wiki/Caesar_cipher

Zad_1a

Koristeći Caesar šifru dekriptirajte sljedeći kriptirani tekst. Hint: tekst je kriptiran s originalnim ključem koji je koristio Julije Cezar.

vljxuqrvw lqirupdflmvnlk vxvwdyd

Možete koristiti Cryptool ili ručno dekriptirati.

Zad_2a

Pretpostavite da za Cezarovu šifru uzmemo ključ 13. Koji bi bio rezultat sljedeće dvostruke kriptografske operacije (nap. koristimo samo engleski jezik):

$$C = E(K, E(K, P)),$$

Gdje je P običan element iz običnog, tj. plaintexta, a K je kriptografski ključ. Napišite odgovor i napravite navedenu dvostruku enkripciju u Cryptool alatu i screenshotajte korake.

Zad_3a

Koliko enkripcijskih koraka je potrebno da bi dobili isti efekt kao u prethodnom zadatku ako bi koristili ključ K = 2?

Zad_4a – monoalfabetska supstitucijska šifra

Ova vrsta šifre slična je Cezarovoj šifri, tj. svako slovo teksta zamjenjuje se drugim slovom abecede, s razlikom što ključ za šifriranje može biti bilo koja permutacija elemenata u otvorenom tekstu. Na ovaj način ključni prostor povećava se sa 26 (u slučaju Cezarove šifre) na 26 !. Ova šifra, međutim, je još uvijek ranjiva na napad koji se temelji na "relativnoj frekvenciji".

https://en.wikipedia.org/wiki/Frequency_analysis)

Vaš zadatak je dekriptirati sljedeći tekst koji koristi monoalfabetsku substitucijsku šifru (svaki element je zamijenjen s drugim elementom

Ivxzoo, Xzvhzi'h xrksvi uzooh rm gsv xzgvtlib lu hfyhgrgfgrlm

nlmlzokszyvgrx xrksvih (r.v., vzxs vovnvmg uiln gsv kozrmgvcg droo

yv ivkozxvw drgs z fmrjfv vovnvmg uiln gsv hkzxv lu xrksvigvcgh).

Uli gsrh ivzhlm, z xrkvsvigvcg kivhvievh gsv ivozgrev uivjfvmxb zg

dsrxs kozrmgvcg vovnvmgh zkkvzi rm gsv xliivhklmwrmt kozrmgvcg. Rm

Evimzn xrksvi, vmxibkgrlm rh kviulinvw yb nvzmh lu vCxofhrev-LI

(CLI) oltrxzo lkvizgrlm (kozrmgvcg rh CLIvw drgs zm vmxibkgrlm

pvb). Ru zm vmxibkgrlm pvb rh xslhvm izmwlnob zmw rh zg ovzhg zh

olmt zh gsv kozrmgvcg gl yv vmxibkgvw, CLI vmxibkgrlm (lmv-grnv

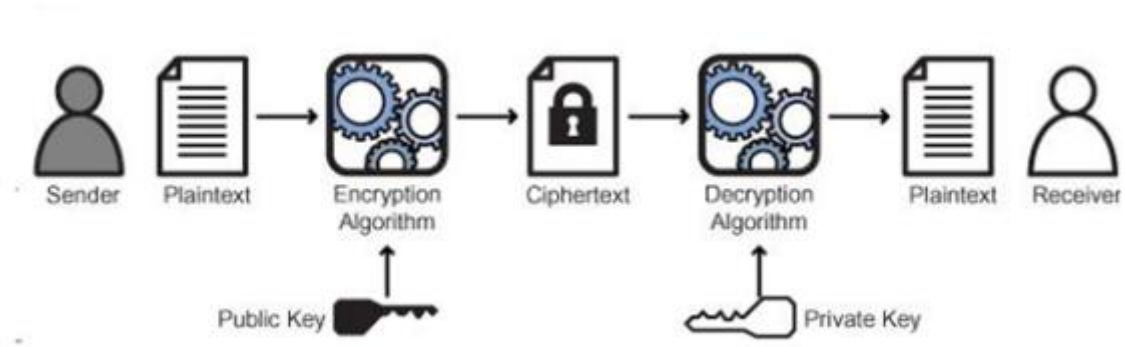
kzw) rh kilezyob (kviuvxgob) hvxfiv.

Za rješenje zadatka koristite Cryptool (šifrirani tekst u novi dokument, pa Analysis> Sym. Enc. (classic)>Manual Analysis > Substitution…) i napravite kriptoanalizu teksta gore imajući u vidu da je prva riječ u šifriranom tekstu, u običnom, tj. plaintext-u riječ ***„Recall"***.

Priložite screenshot rješenja.

Asimetrična kriptografija

Kriptografija javnog ključa (PKC, tj. I), poznata i kao asimetrična kriptografija, okvir je koji koristi i privatni i javni ključ, za razliku od jedinstvenog ključa koji se koristi u simetričnoj kriptografiji. Upotreba parova ključeva daje PKC-u jedinstven skup karakteristika i mogućnosti pomoću kojih se mogu riješiti izazovi svojstveni drugim kriptografskim tehnikama. Ovaj oblik kriptografije postao je važan element moderne računalne sigurnosti, kao i kritična sastavnica rastućeg ekosustava kriptovaluta.



Na koji način radi?

U PKC shemi, javni ključ pošiljatelj koristi za šifriranje podataka, dok privatni ključ primalac koristi za dešifriranje podataka. Kako se dva ključa međusobno razlikuju, javni se ključ može sigurno dijeliti bez ugrožavanja sigurnosti privatnog. Svaki par asimetričnih ključeva je jedinstven, osiguravajući da poruku šifriranu pomoću javnog ključa može pročitati samo osoba koja posjeduje odgovarajući privatni ključ.

Budući da algoritmi za asimetrično šifriranje generiraju ključne parove koji su matematički povezani, njihova duljina ključa je puno duža od one koja se koristi u simetričnoj kriptografiji. Ova veća dužina - obično između 1,024 i 2,048 bita - izuzetno je teško izračunati privatni ključ od njegovog javnog ključa. Jedan od najčešćih algoritama za asimetrično šifriranje koji se danas koristi je RSA.

Kod RSA, ključevi se generiraju pomoću modula do kojeg se dolazi množenjem dva broja (često dva velika jednostavna broja). U osnovi, modul generira dva ključa (jedan javni koji se može dijeliti i jedan privatni koji bi trebao biti čuvan u tajnosti). Algoritam RSA prvi su put opisali 1977. godine Rivest, Shamir i Adleman (otuda, RSA) i ostaje glavna komponenta kriptografskih sustava javnih ključeva.

PKC kao alat za kriptiranje i digitalne potpise

Kriptografija javnog ključa rješava jedan od dugogodišnjih problema simetričnih algoritama, a to je komunikacija ključa koji se koristi i za šifriranje i za dešifriranje. Slanje ovog ključa preko nesigurne veze predstavlja ogroman rizik da ga se izloži trećim osobama, koje mogu čitati sve poruke šifrirane zajedničkim ključem. Iako za rješavanje ovog problema postoje kriptografske tehnike (poput protokola razmjene ključeva Diffie-Hellman-Merkle), one su još uvijek podložne napadima. Nasuprot tome, u kriptografiji javnog ključa ključ koji se koristi za šifriranje može se sigurno dijeliti preko bilo koje veze. Kao rezultat, asimetrični algoritmi nude višu razinu zaštite u odnosu na simetrične.

Druga primjena asimetričnih algoritama kriptografije je provjera autentičnosti podataka pomoću digitalnog potpisa. U osnovi, digitalni potpis je hash kreiran pomoću podataka u poruci. Kad je ta poruka poslana, primalac može provjeriti potpis koristeći javni ključ pošiljatelja. Na taj način mogu potvrditi izvor poruke i osigurati da ona nije ugrožena. U nekim se slučajevima digitalni potpisi i šifriranje primjenjuju zajedno, što znači da se i sam hash može šifrirati kao dio poruke. Međutim, treba napomenuti da sve sheme digitalnog potpisa ne koriste tehnike šifriranja.

Ograničenja i primjene

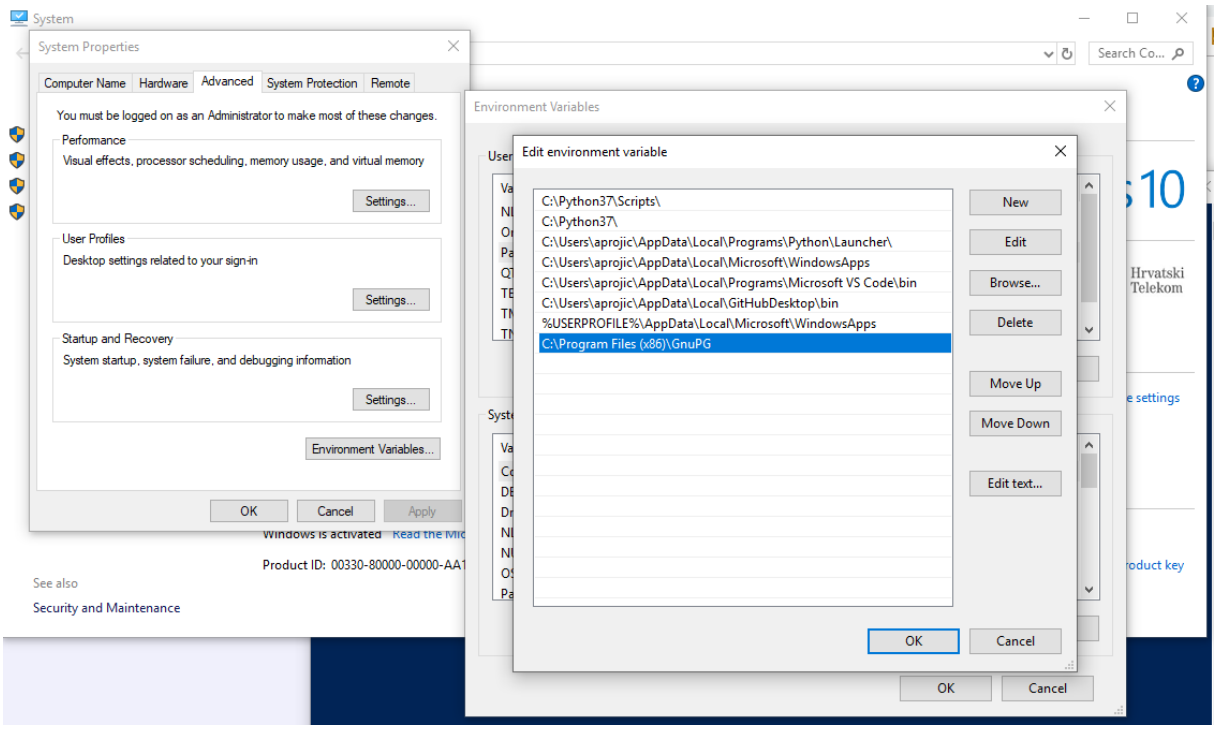
Iako se može koristiti za unapređenje računalne sigurnosti i provjeru integriteta poruke, PKC ipak ima određena ograničenja. Zbog složenih matematičkih operacija uključenih u šifriranje i dešifriranje, asimetrični algoritmi mogu biti prilično spori kada su prisiljeni na obradu velike količine podataka. Ova vrsta kriptografije jako ovisi i o pretpostavci da će privatni ključ ostati tajna. Ako se privatni ključ slučajno podijeli ili izloži, bit će ugrožena sigurnost svih poruka koje su šifrirane odgovarajućim javnim ključem. Korisnici

također mogu slučajno izgubiti svoje privatne ključeve, u tom slučaju im postaje nemoguće pristupiti šifriranim podacima.

Mnogo modernih računalnih sustava koriste ovu vrstu kriptografije za sigurnost osjetljivih informacija. E-poruke, na primjer, mogu se kriptirati pomoću kriptografskih tehnika javnog ključa kako bi se njihov sadržaj održao povjerljivim. Protokol sigurnog utičnice (SSL) koji omogućuje sigurne veze s web stranicama također koristi asimetričnu kriptografiju.

ZADACI

Instalirajte program GNUPG (https://www.gnupg.org). Koristite Windows binaries; dodajte executable u path varijablu (advanced system settings > enviroment variables) da bi se moglo pokretati bez navođenja pune putanje. Npr:



Iz Powershella ili CMD-a vam mora raditi ova naredba:

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --help
gpg (GnuPG) 2.2.17
libgcrypt 1.8.4
Copyright (C) 2019 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

SIMETRIČNA KRIPTOGRAFIJA POMOĆU GNUPG SUSTAVA

Kreirajte datoteku imena koje želite s porukom koju želite. Obavezno navesti vaše ime u tom tekstualnom dokumentu.

Npr:

```
PS C:\Users\aprojic\Desktop\Lab_no1> type .\Poruka.txt
Ovo je tajna poruka
```

Ukoliko želimo kriptirati datoteku pomoću jednog ključa koristimo jednostavnu naredbu:

- Sustav će tražiti enkripcijski ključ (stavite vaše ime)

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --symmetric .\Poruka.txt
PS C:\Users\aprojic\Desktop\Lab_no1> type .\Poruka.txt
Ovo je tajna poruka
PS C:\Users\aprojic\Desktop\Lab_no1> type .\Poruka.txt.gpg
Ś
▯▯▯▯¦f▯‰×▯ĺĂÑO▯őŚ#▯d˝}.+Pţé▯ţ▯&°ťł)Ń6 sa'ÍÁRd‘ó±ĐI[7Ô<˝T ▯Ş¬Ľ¦ á▯▯Fjd'Gű▯x▯ŁŤd▯;Ďy▯çVçH$šš{wS
```

Morate dobiti poruku sličnu kao što je gore. S obzirom da je poruka u binarnom formatu ne možemo je kopirati i poslati. Ukoliko je želimo prikazati u tekstualnom formatu, moramo je kodirati.

Npr.

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --symmetric --armor .\Poruka.txt
PS C:\Users\aprojic\Desktop\Lab_no1> type .\Poruka.txt.asc
-----BEGIN PGP MESSAGE-----

jA0EBwMCOCjKIi4zaH7D0k8BVPgACYPDgZ/6ZzLz8yYv5qild3qm4Ji7IWDwY20j
FR1IzZLxp+h+H3HWc/EZXL2UukehcFan+UuogyGpQiF6SnFsrna7pQTVJDscbQc3
=dMbS
-----END PGP MESSAGE-----
```

Sada se npr. ta poruka može poslati e-mailom, IM-om, itd.

Dekripcija poruke je jednostavna:

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --decrypt .\Poruka.txt.asc
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
Ovo je tajna poruka
PS C:\Users\aprojic\Desktop\Lab_no1>
```

Ukoliko dekriptiranu poruku želimo spremiti u datoteku radimo sljedeće (potrebno ukoliko je poruka bila binarna, tj. slika, word dokument, itd.):

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --out dektriptirana_poruka.txt --decrypt .\Poruka.txt.asc
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
PS C:\Users\aprojic\Desktop\Lab_no1> type .\dektriptirana_poruka.txt
Ovo je tajna poruka
```

VAŽNO: ENKRIPTIRANA i DEKRIPTIRANA DATOTEKA MORA BITI PRILOŽENA OVOJ VJEŽBI KAO I SCREENSHOTOVI SVIH KORAKA.

ASIMETRIČNA KRIPTOGRAFIJA POMOĆU GNUPG SUSTAVA

Za razliku od simetrične kriptografije gdje koristimo samo jedan ključ, kod asimetrične kriptografije svaka strana ima dva ključa. Jedan nazivamo privatni, ili tajni ključ, dok drugi nazivamo javni ključ. Ta dva ključa su u matematičkoj vezi i ukoliko koristimo jedan ključ za kriptiranje, sa drugim je moguće dekriptirati poruku.

Generirajte par ključeva da bi mogli koristiti asimetričnu kriptografiju.

Npr:

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --gen-key
gpg (GnuPG) 2.2.17; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Ante Projić
Email address: anteprojic@gmail.com
You are using the 'CP852' character set.
You selected this USER-ID:
    "Ante Projić <anteprojic@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: C:/Users/aprojic/AppData/Roaming/gnupg/trustdb.gpg: trustdb created
gpg: key 4B235B4838AA9B29 marked as ultimately trusted
gpg: directory 'C:/Users/aprojic/AppData/Roaming/gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as 'C:/Users/aprojic/AppData/Roaming/gnupg/openpgp-revocs.d\9A75ABA8B9
E817546E98A1664B235B4838AA9B29.rev'
public and secret key created and signed.

pub   rsa2048 2019-10-21 [SC] [expires: 2021-10-20]
      9A75ABA8B9E817546E98A1664B235B4838AA9B29
uid                      Ante Projić <anteprojic@gmail.com>
sub   rsa2048 2019-10-21 [E] [expires: 2021-10-20]

PS C:\Users\aprojic\Desktop\Lab_no1>
```

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2021-10-20
C:/Users/aprojic/AppData/Roaming/gnupg/pubring.kbx
-------------------------------------------------
pub   rsa2048 2019-10-21 [SC] [expires: 2021-10-20]
      9A75ABA8B9E817546E98A1664B235B4838AA9B29
uid           [ultimate] Ante Projić <anteprojic@gmail.com>
sub   rsa2048 2019-10-21 [E] [expires: 2021-10-20]

PS C:\Users\aprojic\Desktop\Lab_no1>
```

Export tajnog ključa na lokaciju:

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --armor --export-secret-keys --out tajni
PS C:\Users\aprojic\Desktop\Lab_no1> ls .\tajni


    Directory: C:\Users\aprojic\Desktop\Lab_no1


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       21.10.2019.     16:34           3711 tajni
```

Export vlastitog javnog ključa na lokaciju:

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --armor --out javni --export anteprojic@gmail.com
PS C:\Users\aprojic\Desktop\Lab_no1> ls .\javni


    Directory: C:\Users\aprojic\Desktop\Lab_no1


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       21.10.2019.     16:36           1795 javni


PS C:\Users\aprojic\Desktop\Lab_no1> type .\javni
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBF2tvxABCADEtmNf6r3STw9oH1511O0Rgy0VzKtw/udIrZsq4BE+rXNMkilk
qh96fR2yw8bt3t801ydX4QD2PN2yGWNYbduaOs1XWBLAYHHTA4jeWjNXsyId6G5v
7xh70XA0ADu7uP52QtUdy1IE109jvpMidBNMAqCnxVaIZMoujZbE+YUgTwh36JMR
qc3iFGBNEj7I1YXRpuAPionZA1vaH1tJBZ1Q3UQWCc1xbJ0OPzA73ccg4V/xcKL7
yDpo+95jTTnVkU0GHfeP0kIEjWuFI5u1Lpb+G38taabtxauoAZ5uVn1W7k/j/8Sb
/yEcptE9tFq43kCM1Aaj3dd10tAuMjdPx10dABEBAAG0I0FudGUgUHJvamnEhyA8
YW50ZXByb2ppY0BnbWFpbC5jb20+iQFUBBMBCAA+FiEEmnWrqLnoF1RumKFmSyNb
SDiqmykFAl2tvxACGwMFCQPCZwAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ
SyNbSDiqmyme6wf+I58iKOBuNZdggxRgmATYIi0mfdftMCMEy83ak3IzqKjIMR5+
aJLk3DDx0wZx0B4QRvznsTKJ9MWd8tx5yKf5MR5PTpQHRsiFtofpM8F5err8nN1C
AKuHEAg3kcciu4Zp8rllJ8BK/R3MH/XzRT+0OwLvsYWAEhSdlA1O7BdWDsmv35A1
qVcfzKgv10XWxz02utxFEuzWMdAwLaLlKiB2K3DbrYmbyocETKjp7p0/kPBgvRrA
gqyU5SH4Ip03B8HnDUHyuyuYR3YZZppRUwVokAbzkIPGiPIyYG9etPQaUqT/tx3U
pYYKiqu8P6X8XajxJH3btGkqBUMRhzSD/hTkjLkBDQRdrb8QAQgAuVjYMfzUh1IC
cWYVhF6UYOPuKQ4QZJe2uAXIc2iswuA8r88Mem6hb7/LtDhNsaZvMgUExRnp/+XM
xQl1BEJw+VmA1/+sRJuoKMKWtB/8xw6PNw0hF4pOnfjZn1PF01K/S0gPNPPDYhV8
NhSh51iyNeR8KfPNelo/EwHVLdTTZDsvRLQWxXMwW9by4oi3PDTmYizXdHw5xDVe
/AZUO36pmLnEhcj51NSRguuxPxSUxnTcOm6s/N8jpgRu87WqGPWIuVhDKG96nVE1
zw7QnkWj3EwQLiVnutAA86mD+Z+kn/+vKwRDCmZohW2E6D0wIv6685gdk6kNDNSG
yeFUYDEm3QARAQABiQE8BBgBCAAmFiEEmnWrqLnoF1RumKFmSyNbSDiqmykFA12t
vxACGwwFCQPCZwAACgkQSyNbSDiqmyl48gf/RtV5ca/jZz7jFECdb9ujNZQKRVj9
guwaf9E/87P0IB0IWII8evP6b6UXrwc2cyFuvK01fGjk9Dh/kSXeZGJd46cdinN4
2PtAQCbcc5AF+Cijnbnxx2FaD+NnUwou7bbp4IeDX57WbGHVOvDTXBu+YCUjKwsp
rLCNom5wJMSepw3uFtvW15np/H9JWJqV5R5R/buB5z2i827QuSi7P266x2Kxajml
ylGWzu9qyp64py1+SGApzGsD579ihXK146iY/gL5WYxVWuKd4kb32ZJXVNPRRD1o
Ye5T6OdZZIYnv2tUrfipnT5HRx1zWRrp0XD8LmE4nPXOQhkSX0dHi+XTMA==
=oGeh
-----END PGP PUBLIC KEY BLOCK-----
```

Slanje:

- Ukoliko želite meni poslati poruku morate imate moj javni ključ. Spremite ga u neki dokument.

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

mQENBF2tvxABCADEtmNf6r3STw9oH1511O0Rgy0VzKtw/udIrZsq4BE+rXNMkilk
qh96fR2yw8bt3t80lydX4QD2PN2yGWNYbduaOslXWBLAYHHTA4jeWjNXsyId6G5v
7xh70XA0ADu7uP52QtUdy1IE109jvpMidBNMAqCnxVaIZMoujZbE+YUgTwh36JMR
qc3iFGBNEj7I1YXRpuAPionZA1vaHltJBZ1Q3UQWCclxbJ0OPzA73ccg4V/xcKL7
yDpo+95jTTnVkU0GHfeP0kIEjWuFI5u1Lpb+G38taabtxauoAZ5uVn1W7k/j/8Sb
/yEcptE9tFq43kCM1Aaj3dd10tAuMjdPx10dABEBAAG0I0FudGUgUHJvamnEhyA8
YW50ZXByb2ppY0BnbWFpbC5jb20+iQFUBBMBCAA+FiEEmnWrqLnoF1RumKFmSyNb
SDiqmykFAl2tvxACGwMFCQPCZwAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ
SyNbSDiqmyme6wf+I58iKOBuNZdggxRgmATYIi0mfdftMCMEy83ak3IzqKjIMR5+
aJLk3DDx0wZx0B4QRvznsTKJ9MWd8tx5yKf5MR5PTpQHRsiFtofpM8F5err8nNlC
AKuHEAg3kcciu4Zp8r11J8BK/R3MH/XzRT+0OwLvsYWAEhSdlA1O7BdWDsmv35A1
qVcfzKgv10XWxz02utxFEuzWMdAwLaLlKiB2K3DbrYmbyocETKjp7p0/kPBgvRrA
gqyU5SH4Ip03B8HnDUHyuyuYR3YZZppRUwVokAbzkIPGiPIyYG9etPQaUqT/tx3U
pYYKiqu8P6X8XajxJH3btGkqBUMRhzSD/hTkjLkBDQRdrb8QAQgAuVjYMfzUhlIC
cWYVhF6UYOPuKQ4QZJe2uAXIc2iswuA8r88Mem6hb7/LtDhNsaZvMgUExRnp/+XM
xQllBEJw+VmAl/+sRJuoKMKWtB/8xw6PNw0hF4pOnfjZn1PF01K/S0gPNPPDYhV8
NhSh51iyNeR8KfPNelo/EwHVLdTTZDsvRLQWxXMwW9by4oi3PDTmYizXdHw5xDVe
/AZUO36pmLnEhcj51NSRguuxPxSUxnTcOm6s/N8jpgRu87WqGPWIuVhDKG96nVEl
zw7QnkWj3EwQLiVnutAA86mD+Z+kn/+vKwRDCmZohW2E6D0wIv6685gdk6kNDNSG
yeFUYDEm3QARAQABiQE8BBgBCAAmFiEEmnWrqLnoF1RumKFmSyNbSDiqmykFAl2t
vxACGwwFCQPCZwAACgkQSyNbSDiqmyl48gf/RtV5ca/jZz7jFECdb9ujNZQKRVj9
guwaf9E/87P0IB0IWII8evP6b6UXrwc2cyFuvK01fGjk9Dh/kSXeZGJd46cdinN4
2PtAQCbcc5AF+Cijnbnxx2FaD+NnUwou7bbp4IeDX57WbGHVOvDTXBu+YCUjKwsp
rLCNom5wJMSepw3uFtvW15np/H9JWJqV5R5R/buB5z2i827QuSi7P266x2Kxajml
ylGWzu9qyp64pyl+SGApzGsD579ihXK146iY/gL5WYxVWuKd4kb32ZJXVNPRRD1o
Ye5T6OdZZIYnv2tUrfipnT5HRx1zWRrp0XD8LmE4nPXOQhkSX0dHi+XTMA==
=oGeh
-----END PGP PUBLIC KEY BLOCK-----
```

Ručno dodavanje javnog ključa druge osobe se radi naredbom:

gpg --import ime_datoteke

DIGITALNI POTPIS:

Da bi potpisali neku poruku koristimo sljedeće;

OBJASNITE ŠTO SE DOGAĐA S VLASTITIM KLJUČEVIMA prilikom potpisivanja

```
PS C:\Users\aprojic\Desktop\Lab_no1> type .\Poruka.txt.asc
-----BEGIN PGP MESSAGE-----

owGbwMvMwMHorRztYbFqtibjGuUkroD8otLsRL2SipLYtYcr/cvyFbJSFUoSs/IS
FQrAUp2MxiwMjBwMsmKKLLNKV6/Y+UI8JG/GwjSYKaxMII0MXJwCMJEJ7Oz//U8F
sR29OinJ97LDxPczUi7f6V468ffm05I6Rya2VJl/vbxx74P7YhH5XzY2Kq5aeHzN
NuWatG1GRQUG9TkVk4P7OEN+OxREnI6zMQiuz3Da55K8TL18zafNn1YKrkg8kHbI
MWyWn3vqba3+0y+cBfe7ODGXpV/+8YopIrTZObG46ZD8uV1tGeefHyj/e9T8kv9p
+wdKS53Pqs+zmvL9zJU3LSI3634IuZaF9LzmWFkzrW/Jwodz1i5w0pt96fzG0v3S
0kXdlSq3/+ZHOfHtZX2+6bxnYjb7xgutH+f/yJoZLzI1IEh9eWa1q/aiRr66juyF
YrdCpr4o1VjX0Rt2Ly3myWbWR60xT4JsFb1YAQ==
=JeVM
-----END PGP MESSAGE-----
```

DA BI GARANTIRALI INTEGRIRET PORUKE I AUTENTIČNOST POŠILJATELJA DIGITALNO POTPISANU DATOTEKU MOŽEMO POSLATI ZAJEDNO S PORUKOM.

Digitalni potpis možemo ugraditi i u samu poruku:

```
PS C:\Users\aprojic\Desktop\Lab_no1> type .\Poruka.txt.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Ovo je tajna poruka
-----BEGIN PGP SIGNATURE-----

iQEzBAEBCAAdFiEEmnWrqLnoF1RumKFmSyNbSDiqmykFA12txBcACgkQSyNbSDiq
myl1UUQgAucjsTRQZenr9j4EzmtW2OFCZvczptHQfEbq9Zf0VywogkeHEGSeBm2nd
HF3i/46gSgK98IQ1fu8FtmrBQ6BBsLgg5smjPHtGw+Y4DfxVyactNUhvSfpyZwcg
Lx6qSGT3M4YQCNsEr5kumX4CF1v/99LkgYS92aSKw6NamfFE5cLTFxkE2tKOon2w
0072Oeh6Y5GY+g0h4AmJvoe65cXvrqRC3jbEw3fex1jsoJFe1QK1GXZ2oWOv+9JH
2YXxeFkm7yt89Sx8C+B2m03wWfU/FiYYEqDVWCK5Lu+eVGd9n9aJ+Cu8rSDBLZ5D
xzMD49JN2yiosnvxvdsPEcDlN+bCIg==
=rtoI
-----END PGP SIGNATURE-----
PS C:\Users\aprojic\Desktop\Lab_no1>
```

Digitalni potpis možemo verificirati ako imamo javni ključ osobe koja je potpisala poruku.

ZADATAK: Verificirajte moju poruku priloženu s ovom vježbom.

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --verify .\Poruka.txt.asc
gpg: Signature made 10/21/19 16:43:35 Central European Daylight Time
gpg:                using RSA key 9A75ABA8B9E817546E98A1664B235B4838AA9B29
gpg: Good signature from "Ante Projić <anteprojic@gmail.com>" [ultimate]
gpg: WARNING: not a detached signature; file '.\Poruka.txt' was NOT verified!
```

ZADATAK:

Da bi kriptirali poruku pošiljatelju moramo imati njegov javni ključ. Moj javni ključ je unutar ove vježbe. Kreirajte novi dokument, napišite mi poruku koja obavezno između ostalog mora sadržavati vaše ime i prezime, enkriptirajte je s mojim javnim ključem tako da joj samo ja mogu pristupiti i pošaljite skupa s ostalim rješenjima iz ove vježbe.

Naredba: gpg --encrypt --armor --recipient anteprojic@gmail.com ime_poruke

Primjer: dekriptiranje vaše poruke s moje strane:

```
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --verify .\Poruka.txt.asc
gpg: Signature made 10/21/19 16:43:35 Central European Daylight Time
gpg:                using RSA key 9A75ABA8B9E817546E98A1664B235B4838AA9B29
gpg: Good signature from "Ante Projić <anteprojic@gmail.com>" [ultimate]
gpg: WARNING: not a detached signature; file '.\Poruka.txt' was NOT verified!
PS C:\Users\aprojic\Desktop\Lab_no1> gpg --decrypt .\Poruka.txt.asc
Ovo je tajna poruka
gpg: Signature made 10/21/19 16:43:35 Central European Daylight Time
gpg:                using RSA key 9A75ABA8B9E817546E98A1664B235B4838AA9B29
gpg: Good signature from "Ante Projić <anteprojic@gmail.com>" [ultimate]
```