





CERT.hr

Sadržaj

1	UVOD)	4
2	OSNO	VE KRIPTOGRAFIJE JAVNOG I PRIVATNOG KLJUČA	5
	2.1 3	ŠIFRIRANJE PORUKA	5
	2.2 1	Digitalno potpisivanje	6
	2.3 1	Problem razmjene ključeva	7
3	KORI	ŠTENJE GNUPG-A KROZ GPG4WIN SUČELJE	8
	3.1 I	Instalacija	8
	3.1 I	INSTALACIJA	8
	3.2 I	KORIŠTENJE	12
	<i>3.2.1</i>	Generiranje javnog i privatnog ključa	<i>12</i>
	3.1 I	INSTALACIJA	8
	3.2 I	KORIŠTENJE	12
	<i>3.2.1</i>	Generiranje javnog i privatnog ključa	12
	<i>3.2.2</i>	Izvoz i uvoz javnih ključeva	16
	3.1 I	INSTALACIJA	8
	3.2 I	KORIŠTENJE.	12
	<i>3.2.1</i>	Generiranje javnog i privatnog ključa	12
	<i>3.2.2</i>	Izvoz i uvoz javnih ključeva	16
	<i>3.2.3</i>	Šifriranje i potpisivanje poruke	19
	3.1 1	INSTALACIJA	8
	3.2 1	KORIŠTENJE	12
	3.2.1	Generiranje javnog i privatnog ključa	12
	3.2.2	Izvoz i uvoz javnih ključeva	16
	3.2.3	Šifriranje i potpisivanje poruke	19
	3.2.4	Dešifriranje i provjera potpisa	24

CERT.hr

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT–a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.



1 Uvod

U današnje vrijeme sve više komunikacije odvija se mrežno, preko Interneta. Takva komunikacija često je nesigurna, a najbolji primjer toga je elektronička pošta čija se razina sigurnosti gotovo uopće nije povisila od 90-tih godina. Upravo zbog tih razloga poželjno je koristiti dodatne alate namijenjene zaštiti komunikacije.

Primjerice, recimo da dvije osobe, Tomislav i Antonio, komuniciraju. Poželjno je da se za njihovu komunikaciju osigura:

- **Tajnost** (eng. *confidentiality*) nitko osim Tomislava i Antonija ne može pročitati njihove poruke.
- **Vjerodostojnost** (eng. *authenticity*) mogućnost da Antonio provjeri da poruka zaista dolazi od Tomislava (i obrnuto), a ne od nekoga tko se lažno predstavlja kao Tomislav.

Kako bi se ta svojstva osigurala, razvijeni su razni kriptografski sustavi, standardi i alati. Jedan od najšire korištenih standarda za osiguravanje tajnosti i vjerodostojnosti poruka je OpenPGP. Najpoznatiji slobodni (eng. *free and open source*) alat koji implementira OpenPGP standard je Gnu Privacy Guard (skraćeno GnuPG ili GPG).

Alat GPG moguće je koristiti na operacijskom sustavu Windows kroz programski paket Gpg4win koji između ostaloga sadržava i grafičko sučelje. Ovaj dokument objasnit će kako koristiti GnuPG kroz Gpg4win programski paket, no način uporabe primjenjiv je općenito na GnuPG i ostale alate koji implementiraju OpenPGP standard.



2 Osnove kriptografije javnog i privatnog ključa

Za korištenje GnuPG-a na siguran i ispravan način, potrebno je razumjeti osnove tzv. asimetrične kriptografije. U asimetričnoj kriptografiji svaka osoba koja sudjeluje u komunikaciji ima dva ključa:

- Javni ključ koji je poznat svima
- **Privatni ključ** koji mora ostati tajan svaka osoba mora dobro paziti da nikad nitko drugi ne sazna njen privatni ključ

U ovom poglavlju bit će dan kratki pregled postupka šifriranja i digitalnog potpisivanja pomoću asimetrične kriptografije. Također, bit će opisan problem sigurne razmjene javnog ključa.

2.1 Šifriranje poruka

Kako bi tajnost komunikacije bila osigurana, potrebno je šifrirati razmijenjene poruke. Najlakše je na primjeru razumjeti kako se asimetričnom kriptografijom šifriraju poruke. Recimo da dvije osobe, Tomislav i Antonio, komuniciraju. Tomislav želi Antoniu poslati poruku "Bok, kako si?" bez da itko drugi sazna njen sadržaj. Kako bi to postigao, Tomislav tu poruku **šifrira**.

Asimetričnom kriptografijom, Tomislav će to napraviti na sljedeći način:

- 1. Tomislav nekako pribavi Antonijev javni ključ
- 2. Zatim, Tomislav napiše poruku "Bok, kako si?" te ju **šifrira Antonijevim javnim ključem**
- 3. Tomislav pošalje tu šifriranu poruku Antoniju
- 4. Antonio primljenu šifriranu poruku **dešifrira svojim privatnim ključem** te ju sada može pročitati

Dijagram na slici Slika 1 vizualno prikazuje postupak šifriranja i dešifriranja poruke iz prethodno navedenog primjera.



Slika 1 -Šifriranje i dešifriranje poruke asimetričnom kriptografijom.

2.2 Digitalno potpisivanje

Šifriranjem poruke riješen je problem tajnosti, no ostaje problem vjerodostojnosti – Antonio želi znati da mu je zaista Tomislav poslao poruku, a ne netko drugi. Kako bi taj problem bio riješen, koristi se postupak digitalnog potpisivanja.

Asimetričnom kriptografijom Tomislav može dokazati da je zaista on poslao poruku na sljedeći način:

- 1. Tomislav poruku **potpisuje svojim privatnim ključem**
- 2. Potpisanu poruku Tomislav pošalje Antoniju
- 3. Antonio pribavi Tomislavov javni ključ
- 4. Antonio, kao i svatko drugi tko je u posjedu Tomislavovog javnog ključa, sada može **provjeriti ispravnost potpisa Tomislavovim javnim ključem** te tako potvrditi da je zaista Tomislav napisao poruku

Dijagram na slici 2 prikazuje prethodno opisani postupak digitalnog potpisivanja poruke te provjere potpisa.



Slika 2 - Potpisivanje i provjera potpisa poruke asimetričnom kriptografijom

Takvu, digitalnu potpisanu poruku Tomislav može i šifrirati Antonijevim javnim ključem kako bi se u isto vrijeme osigurale i tajnost i vjerodostojnost.

2.3 Problem razmjene ključeva

Kod ovakvog sustava javnih i privatnih ključeva postoji problem sigurne razmjene ključa – kako Antonio zna da zaista ima Tomislavov javni ključ, a ne ključ napadača koji se lažno predstavlja kao Tomislav?

Primjerice, Tomislav je objavio svoj javni ključ na svojoj Web stranici. No, napadač Marko zatim preuzima kontrolu nad tom Web stranicom te mijenja objavljeni Tomislavov ključ svojim ključem. Sada, Antonio s Tomislavove Web stranice preuzima Markov javni ključ misleći da je to zapravo Tomislavov ključ. U konačnici, Marko se može lažno predstaviti kao Tomislav u komunikaciji s Antoniom.

Jednostavno rješenje ovog problema je sigurno uspoređivanje otiska (eng. *fingerprint*) ključa, koji je puno manje duljine nego sam javni ključ. Antonio se može uživo naći s Tomislavom te usporediti otisak javnog ključa kojeg je preuzeo s otiskom Tomislavovog javnog ključa. Ako su otisci isti, Antonio može biti siguran da je ključ kojeg je preuzeo zaista Tomislavov ključ. Alternativno, Antonio se ne mora naći uživo s Tomislavom, već mogu taj postupak obaviti i telefonski ili na bilo koji drugi siguran način. Bitno je da se otisak i javni ključ ne razmjenjuju istim komunikacijskim kanalom.

Postoje i drugi načini rješavanja ovog problema koji su složeniji, no imaju neke svoje prednosti. Jedan način je korištenje tzv. infrastrukture javnog ključa (eng. *Public Key Infrastructure*, skraćeno *PKI*) u kojoj treće strane provjeravaju vlasništvo ključeva te ih potpisuju. Drugi način je decentralizacija povjerenja kroz mrežu povjerenja (eng. *web of trust*). Detaljniji opisi ovih sustava izvan su opsega ovo dokumenta, no korisno je znati da postoje.

3 Korištenje GnuPG-a kroz Gpg4win sučelje

GnuPG je slobodna (eng. *free and open source*) implementacija standarda OpenPGP koja je nastala kao pandan komercijalnim alatima koji implementiraju taj standard. Najpoznatiji takav komercijalni alat je PGP (skraćeno od eng. *Pretty Good Privacy*), iz kojeg je i nastao OpenPGP standard.

U ovom poglavlju bit će opisan primjer korištenja GnuPG alata na operacijskom sustavu Windows kroz Gpw4win. Gpg4win je skup alata koji uključuje GnuPG i grafičko sučelje za njegovo korištenje.

3.1 Instalacija

1. Za preuzimanje paketa Gpg4win na računalo, potrebno je otvoriti <u>službene</u> <u>stranice</u> alata te pritisnuti na zelenu *Download* tipku.





2. Nakon što je datoteka preuzeta i pokrenuta, pojavit će se okvir za odabir jezika. Kako ne postoji prijevod na hrvatski jezik, u ovom dokumentu upute su napisane za engleski jezik. Potrebno je pritisnuti *OK* za nastavak instalacijskog procesa.



3. Za sljedeći korak potrebno je pritisnuti *Next*.





4. U ovom koraku potrebno je odabrati komponente paketa Gpg4win koje će biti instalirane na računalo. Važno je da bude odabran i alat *Kleopatra* koji će se koristiti u nastavku dokumenta. *Kleopatra* je grafičko sučelje i upravlja ključevima.

🔒 Gpg4win Setup		– 🗆 X
Gpg4win	Choose Components Choose which features of (Gpg4win you want to install.
Check the components you install. Click Next to contin	u want to install and uncheck t ue.	he components you don't want to
Select components to insta	all: GnuPG Kleopatra GPA GpgOL GpgEX	Description Position your mouse over a component to see its description,
Space required: 92.4MB		
Gpg4win-3,0,3	< Ra	ck Next > Cancel
	00	Content 2 Content

5. Nakon odabira instalacijskog direktorija, pritiskom na tipku *Install* počinje kopiranje datoteka na računalo.





6. Nakon što je instalacija uspješno završena, potrebno je pritisnuti *Next*.



7. Kako bi zatvorili instalacijski program potrebno je pritisnuti *Finish*.





3.2 Korištenje

3.2.1 Generiranje javnog i privatnog ključa

Prečac na alat *Kleopatra* može se naći na radnoj površini (eng. *desktop*) računala. Kako na računalu nisu postavljani vlastiti ključevi prvo ih je potrebno generirati. Pritiskom na ikonu s natpisom *New Key Pair* otvara se okvir za generiranje ključeva.

👩 Kleopatra	_	×
<u>File View Certificates Tools Settings Window H</u> elp		
Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Clipboard_		
Welcome to Kleopatra 3.0.2-gpg4win-3.0.3		
Kleopatra is a front-end for the crypto software GnuPG.		
For most actions you need either a public key (certificate) or your own private key.		
 The private key is needed to decrypt or sign. The public key can be used by others to verify your identity or encrypt to you. 		
You can learn more about this on Wikipedia.		
New Key Pair Import		

Potrebno je odabrati *Create a personal OpenPGP key pair*.

	?	×
← Key Pair Creation Wizard		
Choose Format		
Please choose which type you want to create.		
→ Create a personal OpenPGP key pair OpenPGP key pairs are certified by confirming the fingerprint of the	e public ke	ey.
→ Create a personal X.509 key pair and certification re X.509 key pairs are certified by a certification authority (CA). The ge needs to be sent to a CA to finalize creation.	equest enerated r	equest
Next	Ca	ncel



Iako nisu potrebni za rad GPG-a, ime i adresa e-pošte se koriste kako bi se lakše identificirao vlasnik ključa pa ih je svakako poželjno ispravno upisati.

	?	×
← Key Pair Creation Wizard		
Enter Details		
Please enter your personal details below. If you want more parameters, click on the Advanced Settings button.	control ov	er the
Name: Tomislav Tomislavic		(optional)
EMail: tomislav.tomislavic@example.ord		(optional)
Tomislav Tomislavic <tomislav.tomislavic@exam< td=""><td>ple.org></td><td></td></tomislav.tomislavic@exam<>	ple.org>	
4	<u>\</u> dvanced	Settings
Next		<u>C</u> ancel

Pritiskom na *Advanced Settings…* otvara se prozor u kojem je moguće namjestiti postavke ključeva. Odabrane postavke su većinom sigurne, no kao dobru sigurnosnu mjeru poželjno je postaviti i istek ključa na određeni datum pod *Valid until*. U ovom slučaju odabrano je vrijeme od 2 godine.

Advanced Setting	gs - Kleopatra ? X
Key Material	
RSA	2048 bits (default) 🔻
🗸 + RSA	2048 bits (default) 🔻
🔿 DSA	2048 bits (default) 🔻
+ Elgamal	2048 bits (default) 🔻
○ ECDSA	brainpoolP256r1 🔹 🔻
+ ECDH	brainpoolP256r1 💎
Certificate Usage	
Signing	 Certification
Encryption	Authentication
Valid until: 2	2/1/2020 ~



Nakon pritiska na **OK** kako bi se potvrdili odabrani detalji certifikata, pritiskom na **Create** počinje generiranje certifikata.

	?	×
← Key Pair Creation Wizard		
Review Parameters		
Please review the parameters before proceeding.		
Name: Tomislav Tomislavic Email Address: tomislav.tomislavic@example.org		
Show all details		
<u>C</u> reate	C <u>a</u> nce	el

Sada je potrebno odabrati lozinku za privatni ključ. Moguć je rad i bez lozinke, no kako je privatni ključ lagano preuzeti s računala korisnika, lozinka predstavlja važnu sigurnosnu mjeru. Nakon potvrde lozinke potrebno je pritisnuti **OK**.

🔒 pinentry-qt 🛛 🖂							
0	Please enter protect your r	sphrase to /					
	Passphrase:	••••	•••••	Ì			
	Repeat:	••••	••••				
	Quality:		100%				
	ОК		Cancel				



Par javnog i privatnog ključa sada je stvoren. U tekstualnom okviru prikazan je i otisak ključa čija je uloga u sigurnoj razmjeni ključa objašnjena u prethodnom poglavlju.

	?	\times
← Key Pair Creation Wizard		
Key Pair Successfully Created		
Your new key pair was created successfully. Please find deta some suggested next steps below.	ils on the re	esult and
Result		
Key pair created successfully. Fingerprint: EA8B1489D97D3AFBD500C92ED081689540EE	D683	
Next Steps		
Make a Backup Of Your Key Pair		
Send Public Key By EMail		
Upload Public Key To Directory Service		
Einish	<u>C</u> a	incel

U daljnjim primjerima podrazumijeva se da je istovjetan postupak napravljen i na računalu korisnika *Antonio.*



3.2.2 Izvoz i uvoz javnih ključeva

Sada je potrebno dohvatiti i uvesti Antonijev javni ključ u alat *Kleopatra*. To je najlakše napraviti tako da se javni ključ pomoću alata *Kleopatra* izveze (eng. *export*) u datoteku koju će tada Antonio poslati Tomislavu. Na Antonijevom računalu u alatu *Kleopatra* potrebno je označiti Antonijev par ključeva te pritisnuti ikonu s natpisom *Export*.

👩 Kleop	atra											-		×
Datoteka	Prikaz Potvrde	Alati	Postavk	e Win	dow	Pomoć								
2	Ľä.			₽\$		Q	Ē							
Sign/Encry	ot Decrypt/Verify	Import	Export	Certify	Look	up on Server	Clipboard,							
Search	<alt+q></alt+q>										All Certifi	cates		•
	Nan	ne					E-Mail	User-IDs	Valid From	Valid Until	Details	Ke	y-ID	
Anto	nio Antonic			1	antoni	o.antonic@	example.org	certified	1.2.2018.		OpenPGP	9138	BDEEF	

Zatim je potrebno upisati ime datoteke te ju spremiti pritiskom na *Save*.

Export Certificates			×
← → * ↑ 📘	> This PC > Desktop > gpg	✓ ັບ Search gpg ,	
Organise 🔻 Ne	w folder		
 ✓ A Quick access Desktop Downloads Documents Pictures antonio A OneDrive This PC Network 	Name No it	Date modified Type ems match your search.	Siz
	<		>
File name:	Antonio_certifikat		~
Save as type:	OpenPGP Certificates (*.asc *.gpg *.pgp)		~
 Hide Folders 		Save Cancel]



Na Tomislavovom računalu potrebno je uvesti (eng. *import*) Antonijev javni ključ. Dvostrukim pritiskom na datoteku s Antonijevim javnim ključem otvara se prozor u kojem je potrebno potvrditi povezanost javnog ključa s osobom Antonio. Pritiskom na **OK** počinje sljedeći korak.

🗊 You have imported a new certificate (public key) ? X							
Ĺ	In order to mark the certificate as valid (green) it needs to be certified. Certifying means that you check the Fingerprint. Some suggestions to do this are:						
	A phone call to the person.						
	Using a business card.						
	Confirming it on a trusted website.						
Do you wish to start this process now?							
Do n	ot ask again						
	√ <u>Y</u> es ⊖ <u>N</u> o						

Nakon što je provjerena podudarnost otiska ključa koji je Antonio poslao i koji je Tomislav primio, potrebno je označiti ime korisnika kojeg želimo potvrditi i kućicu uz *I have verified the fingerprint* te pritisnuti na *Next*.

	?	×
 Certify Certificate: Antonio Antonic 		
Step 1: Please select the user IDs you wish to certify.		
Antonio Antonic <antonio.antonic@example.org></antonio.antonic@example.org>		
Certificate: Antonio Antonic <antonio.antonic@example.org> (9:</antonio.antonic@example.org>	L38DEEF)	
Fingerprint: 6C33D59B8C8744E7AD108833925EF8839138DEEF J have verified the fingerprint		
Next	<u>C</u> anc	el



U sljedećem koraku potrebno je pritisnuti na *Certify* kako bi Tomislav svojim privatnim ključem jamčio povezanost javnog ključa i Antonijevih podataka tj. stvorio certifikat.

	?	×
← Certify Certificate: Antonio Antonic		
Step 2: Choose how to certify.		
Certification will be performed using certificate Tomislav Tomislavic <tomislav.tomislavic@< td=""><td>example</td><td>.org>.</td></tomislav.tomislavic@<>	example	.org>.
Certify only for myself		
Certify for everyone to see		
\checkmark <u>S</u> end certified certificate to server afterwards		
Certify	C <u>a</u> i	ncel

Potvrda ključeva sada je uspješno završena te pritiskom na *Finish* završavamo proces potvrde te možemo koristiti Antonijev certifikat.

		?	\times
- Certify Certificate: Antonio Antonic			
Summary:			
Signed user IDs:	Antonio Antonic <antonio.antonic@exa< td=""><td>mple.org></td><td>•</td></antonio.antonic@exa<>	mple.org>	•
Selected secret key:	Tomislav Tomislavic <tomislav.tomisla< td=""><td>vic@exam</td><td>ple.org></td></tomislav.tomisla<>	vic@exam	ple.org>
	Certification successful.		
	<u>E</u> inish	<u>C</u> a	ncel



3.2.3 Šifriranje i potpisivanje poruke

Ako Tomislav želi Antoniju poslati poruku e-pošte te osigurati njenu tajnost i vjerodostojnost, to može učiniti tako da poruku potpiše svojim privatnim ključem te ju šifrira Antonijevim javnim ključem. Sadržaj tajne poruke prvo je potrebno staviti u međuspremnik (eng. *clipboard*), npr. tako da označimo cijelu poruku te nakon desnog pritiska miša na nju odaberemo *Copy*.

Tajna poruka	_ ~ ×
antonio.antonic@example.org	
Tajna poruka	
Ovo je sadržaj tajne poruke!	
Send <u>A</u> 🛈 🔥 🔟 🖙 😌	Saved 📋 👻

U alatu *Kleopatra* pritiskom na ikonu s natpisom *Clipboard* i odabirom *OpenPGP-Sign…* započinjemo proces digitalnog potpisivanja poruke.

🗊 Kleopatra					— (
<u>File View Certificates Tools Settings</u>	<u>W</u> indow <u>H</u> elp					
Sign/Encrypt Decrypt/Verify Import Export	Certify Lookup on Server	Elipboard,				
Search <alt+q></alt+q>		Certificate Import		AI	l Certificates	•
Name	E-Mail	Encrypt S/MIME-Sign	Ds	Valid From	Valid Until	Details
Tomislav Tomislavic	tomislav.tomislavic@exa	OpenPGP-Sign		2/1/2018	2/1/2020	OpenPGP
Antonio Antonic	antonio.antonic@example	Decrypt/Verify		2/1/2018		OpenPGP
<						>



Sada je potrebno odabrati ključ kojim ćemo potpisati poruku. Taj proces započinjemo pritiskom na *Change Signing Certificates…* .

🗊 Sign Mail Message - Kleopatra			?	×
Choose Operation to be Performed				
Signing Options Sign using OpenPGP: No certificate selected Change Signing Certificates				
You need to select an OpenPGP signing certificate to pro	ceed.			
	Back	Next	Car	icel

Potrebno je odabrati certifikat generiran na početku dokumenta.



Zatim je potrebno upisati lozinku privatnog ključa koja je upisana u procesu generiranja ključeva kako bi poruku mogli potpisati s odabranim privatnim ključem.





U međuspremniku se sada nalazi digitalno potpisana poruka. Za provjeru je možemo zalijepiti kao što je prikazano na donjoj slici:

Tajna poruka	-	2	×
antonio.antonic@example.org			
Tajna poruka			
BEGIN PGP SIGNED MESSAGE Hash: SHA256			
Ovo je sadržaj tajne poruke! BEGIN PGP SIGNATURE			
iQEzBAEBCAAdFiEE6osUidl9OvvVAMku0IFolUDu1oMFAlpyijYACgkQ0IFolUDu 1oNW3wf/TTWejAdBhxrowQLJXeVJ+dRR6YxAJLDuIYDX1ifJJOkqM2NYc/+bKC2A Ycs5DSIKycWP4i8dX4RstTkcDc9AsD0ynmyIupcpwLFLdZV6Ztx2mzJ5qVZ9N8fC pPPzy1ffee6E1pGiOWjtQfSw4oTgXQvXI7zWasIP9wFK1j6JSiBwbayhdMTdc9TU YLV32IRT0Bv7kvioL9/vq4jHiHVPVCdSK5hMqrXXY0S4K9uXb74FRwRAF4Q2YMsU 7yvUiroVk0QMUkkIOXhetVw9apI5dYwi6UhOvKLW1ZEKsEXgmRT/2GVF9Et7DQFq bGeHazTs2qJ19oZt6sBk7t07dXVWsg== =QyA2 END PGP SIGNATURE			
Send A 🛛 🖉 🍋 🖘 😌	Î		Ŧ

Kako bi poruka bila šifrirana, potrebno je opet pritisnuti na ikonu s natpisom *Clipboard*, no ovaj put odabrati "*Encrypt…"*.

🗊 Kleopat	ra								_	
<u>F</u> ile <u>V</u> iew	<u>C</u> ertificates	<u>T</u> ools	<u>S</u> ettings	<u>W</u> indo	w <u>H</u> elp					
Sign/Encrypt	ین Decrypt/Verify	 Impor	■ t Export	E Certify	Q Lookup on Server	E Clipboard				
Search <al< td=""><td>t+Q></td><td></td><td></td><td></td><td></td><td>Certificate Import</td><td></td><td></td><td>All Certificates</td><td>•</td></al<>	t+Q>					Certificate Import			All Certificates	•
	Name				E-Mail	Encrypt	Ds	Valid Fro	m Valid Un	til Details
Tomis	av Tomislavic			tomisla	v.tomislavic@exa	S/MIME-Sign		2/1/2018	2/1/2020	OpenPGP
Antoni	o Antonic			antonio.	antonic@example	Decrypt/Verify		2/1/2018		OpenPGP
<										>



Pritiskom na *Add Recipient…* otvaramo prozor za dodavanje korisnika za kojeg šifriramo poruku.

👩 Encrypt Mail Message - Kleopatra				?	×
Recipients					
Add Recipient Remove Selected					
OpenPGP <u>S</u> /MIME					
	_	_			
	<u>B</u> a	ick	Next	<u>C</u> ar	ncel

Potrebno je odabrati Antonijev ključ, pritisnuti na **OK**, a zatim na **Next**

Encryp	t Mail Message - Kleopatra	?	
cipients			
¢.	Certificate Selection - Kleopatra ?	×	
F	Please select one of the following certificates:		
	Search All Certificates	•	
	Name E-Mail		
	Tomislav Tomislavic tomislav.tomislavic@ex	ample	
	Antonio Antonic antonio.antonic@exampl	e.org	
ld Rec	<u>OK</u> <u>R</u> eload <u>L</u> ookup New Closent	>	
	<u>B</u> ack <u>N</u> ext	<u>C</u> ar	ncel



Pritiskom na **OK** zatvara se prozor za šifriranje sadržaja međuspremnika, te se šifrirana poruka sada nalazi u međuspremniku.

👦 Encrypt Mail Message - Kleopatra			?	×
Results				
All operations completed.				
				100%
Encryption succeeded.				
✓ Keep open after operation completed				
	<u>B</u> ack	√ <u>O</u> K	<u>C</u> a	ncel

Takva šifrirana poruka se može iz međuspremnika zalijepiti u poruku e-pošte:

Tajna poruka 🗅 Inbox x
Tomislav Tomislavic <tomislavic.tomislav@example.org></tomislavic.tomislav@example.org>
to me 🖃
BEGIN PGP MESSAGE
INCENTA40111001115JAQ1+OHVSE01K2DDCJ11GD+G085//11J1J1P05528111116CD10J Dnk7gYotAg4/W//PbFiu+EPtUnd5iUHZGb//LIHEibCBBEOzyHpizCOEo1ApPy/i6u
VK2HJYCXAnoY7ZgmxvXYv5ZdQH+6PGLa1C0AKrg4iHXogitWfL/cG9MnpdE5PTTY
UgUVDmXowibD/NA6xJGk61eM5Fgb0/ZJxjY5MEvbfzc4J7opbVVCoMzPH6k1jt5a
vQKpUevbx4lxoAJY/BGKAoGuYHgPzU1aLvmymVS/AYas5eYpJqA1sIJNui5/7gio
uiAGUZs9TuDdYw9Z5HgVPq8CVVdpdJBU07Y3TdfXqtLBOQHjKGq+ixeUF+8y8Llx
JeZvPGThMzjmvJaA1h1HRyugCNNpxME/brTBB+omo+wmEyOxIF4/vtc3FbEZUOm8
NKDyD8dDPhgm30YDm6ubsAhaBtJvMqoxHzH8kIjzz/XsmA9eNUrAx6HFttx/Fq+N
PICEGSTITITIGO+PDSE+OFIK/VIVG9IWITGUSQUWKQTEGUSXXOFIWIJT/TTXWDS5115 TpMBpEbOkd5V/RW/KKWppc2CpdTKTPwsKL9Mt9clSWt80NiLS8PwXS/Kbay.lwXcdHt
9v/QasnlkRPBOawQQKB5Rab4QQzVmv/PTJCT50VRp64rUAH5pFNT1laMbVZv34+D
+30y2DzaX7pgWdAaVytvl8uq9i7PuLNfYMdseVafdQwDA77uFjd97FqZ/nhc9hrf
OcRzMOGiLVdShSLQSCKnZEeVb9ZvZhZmtZFUZY7ikt047z3C5y2jYUUBzIvYKJh/
e3udxU74bo16lSbWlrhvu43/dtGxeXJBoYdZGisU6rQZiLmLXKWfpAjzSujCTLdO
w4FL68tRsmNNIMJhhJckYut2LwGZASQdg0maE7x1t9dkeeRcK6InIo7pL48eaXSK
TbmADh6X4vR3/rCic9afHpmKW9wiEgBIVLWvTHph2uj9THe3jmjH8ZLbY62I+uB0
END PGP MESSAGE



3.2.4 Dešifriranje i provjera potpisa

Nakon što je korisnik Antonio dobavio Tomislavov javni ključ i potvrdio da je to zbilja javni ključ koji pripada korisniku Tomislav, može dešifrirati i provjeriti ispravnost potpisa poruke. Označavanjem i kopiranjem poruke u međuspremnik taj proces može započeti. Otvaranjem alata Kleopatra te odabirom ikone *Clipboard* i odabirom *Decrypt/Verify…* počinje proces dešifriranja.

📅 Kleopatra Datoteka Prikaz <u>P</u> otvrde <u>A</u> lati P <u>os</u> tavke <u>Wi</u> ndow Po <u>m</u> oć						- 🗆	×
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server	Clipboard, Certificate Import						
Search <alt+q> Name Antonio Antonic antonio.antonic@ Tomislav Tomislavic tomislav.tomislavic</alt+q>	Contracte import Encrypt S/MIME-Sign OpenPGP-Sign Decrypt/Verify	User-IDs certified certified	Valid From 1.2.2018. 1.2.2018.	Valid Until	All Certifi Details OpenPGP OpenPGP	Key-ID 9138DEER 40EED683	

Šifrirana poruka iz međuspremnika je sada dešifrirana te takva spremljena u međuspremnik. Za zatvaranje prozora je potrebno pritisnuti *Finish.*

		?	×
~	Decrypt/Verify E-Mail		
I	Results		
:	Status and progress of the crypto operations is shown here.		
	All operations completed.		
	Clipboard contents \rightarrow Clipboard: Decryption succeeded . Note: You cannot be sure who encrypted this message as it is not signed.		
	<u>F</u> inish	Can	icel



Dešifriranu poruku u međuspremniku moguće je provjeriti tako da otvorimo uređivač teksta u koji možemo zalijepiti sadržaj poruke, kao što je prikazano u donjoj slici:

```
🥘 Untitled - Notepad
                                                                  Х
File Edit Format View Help
----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256
Ovo je sadržaj tajne poruke!
----BEGIN PGP SIGNATURE-----
iQEzBAEBCAAdFiEE6osUid190vvVAMku0IFo1UDu1oMFA1pyijYACgkQ0IFo1UDu
1oNW3wf/TTWejAdBhxrowQLJXeVJ+dRR6YxAJLDu1YDX1if1J0kqM2NYc/+bKC2A
Ycs5DS1KycWP4i8dX4RstTkcDc9AsD0ynmyIupcpwLFLdZV6Ztx2mzJ5qVZ9N8fC
pPPzy1ffee6E1pGi0WjtQfSw4oTgXQvXI7zWas1P9wFK1j6JSiBwbayhdMTdc9TU
YLV32IRT0Bv7kvioL9/vq4jHiHVPVCdSK5hMqrXXY0S4K9uXb74FRwRAF4Q2YMsU
7yvUiroVk0QMUkkIOXhetVw9ap15dYwi6UhOvKLW1ZEKsEXgmRT/2GVF9Et7DQFq
bGeHazTs2qJ19oZt6sBk7t07dXVWsg==
=QyA2
----END PGP SIGNATURE-----
<
```

Ponavljanjem odabira *Decrypt/Veryfy* u alatu Kleopatra sada možemo provjeriti tko je digitalno potpisao poruku. Pokazuje se poruka da je poruka potpisana privatnim ključem koji odgovara javnom ključu korisnika Tomislav.





4 Zaključak

Ovaj dokument dao je kratki teoretski uvod u asimetričnu kriptografiju, javne i privatne ključeve te postupak šifriranja i digitalnog potpisivanja pomoću njih. Asimetričnom kriptografijom moguće je osigurati tajnost i vjerodostojnost poruka poslanim preko nesigurnih medija kao što je elektronička pošta.

Korištenjem ovih uputa moguća je praktična primjena asimetrične kriptografije alatom GnuPG na operacijskom sustavu Windows kroz programski paket Gpg4win. Korištenje alata opisano je na primjeru zaštite teksta elektroničke pošte, no GnuPG i Gpg4win je moguće primijeniti općenitije, primjerice i na zaštitu datoteka.

Postoje alati, primjerice dodaci za Web preglednike i dodaci za klijente e-pošte, koji djelomično automatiziraju proces prikazan u ovom dokumentu, no oni u suštini obavljaju isti postupak. Postupak opisan u ovom dokumentu dovoljan je za sigurno korištenje alata Gpg4win te je koristan i za općenito razumijevanje alata koji za zaštitu komunikacije koriste OpenPGP standard.