Nastavni predmet:	**SIGURNOST INFORMACIJSKIH SUSTAVA**
Vježba: 01	Zaštita pristupa datotekama, direktorijima i diskovima metodom enkripcije
Cilj vježbe:	Upoznati učenike s zaštitom pristupa datotekama, direktorijima i diskovima metodom enkripcije

PRIPREMA ZA VJEŽBU

Proučiti osnove kriptografije, simetrične i asimetrične kriptografske algoritme te kriptografske algoritme za računanje sažetaka. Proučiti zaštitu pristupa datotekama, direktorijima i diskovima pomoću enkripcije.

IZVOĐENJE VJEŽBE

Postupke, korištene naredbe i dobivene rezultate zadataka zapisivati u bilježnicu te odgovoriti na postavljena pitanja vezana uz vježbu.

Zadatak 1: Certifikati

Pokrenuti Windows operacijski sustav.

Ulogirati se kao korisnik koji ima administratorske ovlasti.

U korijenskom direktoriju **podatkovne** particije kreirati direktorij **SIS_LV01**.

a) Kreirati korisnika **ENKRIPCIJA**.

Pokrenite komandnu liniju s **administratorskim ovlastima**:

U Windows tražilicu upisati cmd->desni klik na cmd->odabrati Run as administrator

U komandnu liniju upisati naredbu:

net user ENKRIPCIJA /ADD

U komandnu liniju upisati naredbu:

net user

Da li je stvoren novi korisnik?

Stvorenom korisniku **ENKRIPCIJA** dodijelite lozinku **aes**

net user ENKRIPCIJA *

(potvrdite dodijeljenu lozinku)!

Pogledajte trenutne postavke stvorenog računa **ENKRIPCIJA**:

net user ENKRIPCIJA

b) U komandnu liniju upišite naredbu **certmgr**.

Što se dogodilo?

Uočite da za otvoreni prozor piše slijedeće:
certmgr – [Certificates – Current User]

Pozicionirajte se u:

Certificates – Current User->dvoklik na Personal

Postoji li kakav objekt tj. certifikat?

Zatvorite prozor **[Certificates – Current User]**.

Izaći iz komandne linije naredbom **exit**.

c) Stvoriti korisnike **TEST1**, **TEST2** i **TEST3** ako **VEĆ NE POSTOJE**!

Zadatak 2: Enkripcija

a) Ulogirati se kao korisnik **ENKRIPCIJA**.

Pozicionirajte se u direktorij **SIS_LV01.**

Kreirajte tekstualnu datoteku **enkr.txt** i unestie proizvoljni tekst u stvorenu datoteku.

Pogledati da li je i datoteka **enkr.txt** naslijedila sva prava za sve korisnike:

enkr.txt ->Properties->odabrati tab Security

b) Da bi enkriptirali datoteku **enkr.txt** pozicionirajte se u:

enkr.txt ->Properties->General tab->Advanced

Kvačicom označite opciju **Encrypt contents to secure data**.

Kliknuti **Ok**, pa **Apply**.

Što se dogodilo?

U bilježnicu zapišite ponuđeni odabir!

Odabrati opciju **Encrypt the file only**.

Kliknuti **Ok.**

c) Ako se u donjem desnom kutu ekrana pojavilo upozorenje (notification) naziva **Back up your file encryption key** pročitajte njegov sadržaj.

U bilježnicu odgovorite što se može dogoditi ako ne napravimo pohranu (back up) **FEK**-a?

Uočite da je datoteka **enkr.txt** dobila **oznaku lokota na svojoj ikoni!**

Pokušajte pročitati i izmijeniti sadržaj datoteke. Da li se uspjeli?

d) Pokrenite komandnu liniju i upišite naredbu **certmgr**.

Pozicionirajte se u:

Certificates – Current User->dvoklik na Personal->dvoklik na Certificates

Postoji li sada kakav certifikat?

Ako postoji zapišite u bilježnicu četiri podatka vezana za taj cetrifikat:

Issued to:

Issued by:

Expiration Date:

Intended Purposes:

e) Ulogirati se kao korisnik **TEST1:**

Kliknuti na **Win tipku**->Desni klik na ikonu korisnika->**Odabrati korisnika TEST1**.

Ulogirati se!

Pozicionirajte se u direktorij **SIS_LV01.**

Pokušajte pročitaiti i izmijeniti sadržaj datoteke **enkr.txt.**

Da li ste uspjeli?

f) Ulogirati se kao **korisnik koji ima administratorske ovlasti**.

Pokušajte sada pročitaiti i izmijeniti sadržaj datoteke **enkr.txt**.

Da li ste uspjeli?

g) U direktoriju **SIS_LV01** kreirajte poddirektorij **Kopija.**

Kopirajte datoteku **enkr.txt** u poddirektorij **Kopija**.

Ako se pojavi poruka **You'll need to provide administrator permission to copy this file** iskoristite svoja administratorska prava i kliknite na **Continue**.

Da li ste uspjeli kopirati datoteku?

U bilježnicu napišite što se dogodilo!

Zadatak 3: Kreiranje certifikata i ključa

a) Ulogirati se kao korisnik **ENKRIPCIJA**.

Pokušajte korisniku **TEST2** dodijeliti mogućnost pristupa datoteci **enkr.txt**.

Pozicionirajte se u direktorij **SIS_LV01.** Odaberite:

enkr.txt ->Properties->General Tab->Advanced->Details->Add

Pojavit će se prozor naziva Windows security.

Možete li odabrati korisnika **TEST2**?

Uočite da drugi korisnici moraju imati tražene certifikate da bi ih mogli dodati u listu za pristup datoteci!

b) Za korisniika **TEST2** treba kreirati certifikat za enkripciju datoteke.

Ulogirati se kao korisnik **TEST2.**

U Windows tražilicu upisati:

Certificates

Odabrati **Manage file encryption certificates.**

Kliknite **Next**.

Odabrati **Create a new certificate** te kliknuti **Next**.

Odabrati **Make a new self-signed certificate and store it on my computer** te kliknuti **Next**.

Odabrati **Back up later** te kliknuti **Next**.

Odabrati **I'll update my encrypted files later** i kliknuti **Next**.

Kliknite na **View Certificate** i pogledajte što je sve navedeno!

Kliknuti **Ok** te kliknuti **Close**.

Kliknuti na **Start**.

Iz komandne linije pokrenuti certmgr.

Pozicionirajte se u:

Certificates – Current User->dvoklik na Personal->dvoklik na Certificates

Da li je kreiran certifikat za enkripciju datoteke?

c) Ulogirati se kao korisnik **ENKRIPCIJA**.

Korisniku **TEST2** dodijeliti mogućnost pristupa datoteci **enkr.txt**.

Pozicionirajte se u direktorij **SIS_LV01**. Odaberite:

enkr.txt ->Properties->General Tab->Advanced->Details->Add

Odabrati korisnika **TEST2**. Kliknuti **Yes** i **OK**.

d) Ulogirati se kao korisnik **TEST2.**

Pokušajte pristupiti datoteci **enkr.txt** te izmijeniti njezin sadržaj.

Da li ste uspjeli?

e) Da ste umjesto ovog postupka kao korisnik **TEST2** na svom korisničkom računu stvorili neku novu datoteku i enkriptirali ju da li bi dobili certifikat za enkripciju datoteke?

Da li bi tada korisnik **ENKRIPCIJA** mogao dodati korisnika **TEST2** u listu za pristup enkriptiranoj datoteci **enkr.txt**?

Odgovorite u bilježnicu na ova dva pitanja!

Zadatak 4: Pohrana certifikata i ključa

a) Ulogirati se kao korisnik **ENKRIPCIJA**.

U direktoriju **SIS_LV01** kreirajte poddirektorij **Kljuc.**

U poddirektoriju **Kljuc** kreirati datoteku **kljuc.txt**.

Kao sadržaj datoteke **kljuc.txt** upisati:

Ovo je datoteka za pohranu!

b) Pozicionirati se na poddirektorij **Kljuc** te ga enkriptirati.

Kljuc-> Properties->General tab->Advanced

Kvačicom označite opciju **Encrypt contents to secure data**.

Kliknuti **Ok**, pa **Apply**.

Odabrati **Apply changes to this folder, subfolders and files**.

Kliknuti **Ok**.

Provjerite možete li pristupiti i datoteci **kljuc.txt** unutar enkriptiranog poddirektorija **Kljuc**.

c) Napraviti pohranu certifikata i ključa.

Iz komandne linije pokrenuti certmgr.

Pozicionirajte se u:

Certificates – Current User->dvoklik na Personal->dvoklik na Certificates

Pozicionirajte se na certifikat **ENKRIPCIJA**.

Desni klik->All Tasks->Export

Kliknuti **Next**.

Odabrati opciju **Yes, export the private key** te kliknuti **Next**.

Odabrati opciju **Personal Information Exchange – PKCS #12 (.PFX)** te kliknuti **Next**.

Uočite da u donjem lijevom kutu piše **Encryption: TripleDES-SHA1**

Kakav je **TripleDES**, a kakav **SHA1** algoritam?

Da li u danjašnje vrijeme spadaju u snažnije ili slabije algoritme?

Odgovoriti u bilježnicu!

Stavite kvačicu na Password i unesite lozinku: **privatnikljuc**.

Potvrdite unesenu lozinku!

Kliknite **Next.**

Kao mjesto pohrane ključa odabrati direktorij **SIS_LV01**.

Pohraniti pod imenom **Mojkljuc**.

Kliknuti **Save**.

Provjeriti željeni put za pohranu ključa.

Kliknuti **Next** te **Finish**.

Trebala bi se pojaviti poruka: **The Export was successful**.

Da li je u direktoriju **SIS_LV01** pohranjen ključ pod imenom **Mojkljuc**.

Ovaj ključ može se pohraniti na neki od medija za pohranu podataka (CD, DVD, usb). Može dobro doći ako korisnik **ENKRIPCIJA** zaboravi lozinku svog korisničkog računa.

Zadatak 5: Ključevi i korisnička lozinka

Zamislite slučaj da je korisnik **ENKRIPCIJA** zaboravio svoje korisničko ime.

Administrator bi mu morao dodijeliti novu lozinku.

Ako administrator kreira novu lozinku da li bi korisnik **ENKRIPCIJA** mogao pristupiti datoteci **kljuc.txt**?

a) Odlogirati se kao korisnik ENKRIPCIJA.

Ulogirati se kao korisnik koji ima administratorske ovlasti!

Korisniku **ENKRIPCIJA** dodijelite novu lozinku!

U Windows tražilicu upisati Control panel.

Kliknuti na **User accounts**.

Opet kliknuti na **User Accounts**.

Odabrati **Manage another account->kliknuti na korisnika ENKRIPCIJA**

Odabrati **Change the password!**

Unijeti novu lozinku:

tkip

Potvrditi lozinku (**tkip**) i izvesti promjenu.

b) **Resetirati računalo!**

Ulogirati se kao korisnik **ENKRIPCIJA**.

Pozicionirati se u poddirektorij **Kljuc** i pogledati sadržaj datoteke **kljuc.txt**.

Što se dogodilo s ključem prilikom promjene lozinke?

Kako bi pogledali sadržaj datoteke **kljuc.txt**?

c) Treba vratiti pohranjeni ključ (back up) pomoću datoteke **Mojkljuc** koja se nalazi u direktoriju **SIS_LV01**.

Pozicionirati se u direktorij **SIS_LV01.**

Dvokilik na datoteku Mojkljuc!

Kliknuti **Next**, pa opet **Next**.

Unesite lozinku:

privatnikljuc

Odabrati i opciju **Mark this key as exportable** te kliknuti **Next**.

Odabrati opciju **Automatically select the certificate store based on the type of certificate** te kliknuti **Next**.

Kliknuti **Finish**.

Koja se poruka napisala?

d) Pokušati sada pristupiti datoteci **kljuc.txt** u poddirektoriju **Kljuc**.

Da li ste uspjeli? Zašto?

Zadatak 6: VeraCrypt

VeraCrypt je aplikacija za uspostavu i održavanje enkripcije Windows datotečnih sustava.

Podaci pohranjeni unutar kriptiranog datotečnog sustava ne mogu se pročitati (dekriptirati) bez poznavanja ispravne lozinke ili posjedovanja ispravnog ključa.

a) Ulogirati se kao korisnik koji ima administratorske ovlasti.

Prije same instalacije pozvati nastavnika!

Kreirati **poddirektorij VCrypt** u direktoriju **SIS_LV01**.

b) Instalirati aplikaciju **VeraCrypt**.

Pokrenite **VeraCrypt Setup 1.18a.exe**.

Označiti **I accept the license terms**, kliknuti **Next**.

Odabrati **Install**, pa **Next**.

Instalirati aplikaciju u **poddirektorij VCrypt** koji se nalazi u direktoriju **SIS_LV01**.

Kliknuti **Browse** i odabrati poddirektorij **VCrypt.**

Ostaviti označene sve ponuđene opcije.

Kliknuti **Install**.

Kliknuti **Ok** i zatim **Finish**.

Na upit želite li pogledati tutorijal kliknite **No**.

c) Pokrenite **VeraCrypt** (Kliknite na ikonu).

Odabrati **drive V:** i kliknuti na **Create Volume**.

Odabrati **Create an encrypted file container** opciju, pa **Next**.

Odabrati **Standard VeraCrypt Volume**, pa **Next**.

Kliknuti na **Select file**.

Pozicionirati se u direktorij **SIS_LV01** i pod File Name upisati **Vera** (Save as type: All files).

Još jednom provjerite što ste odabrali i pročitajte upute!

Kliknuti **Next**.

Encryption Algorithm ostaviti **AES**. I ostale postavke ostaviti iste. Kliknuti **Next**.

Volume Size odabrati: **100 MB**. Kliknuti **Next**.

Upisati Password **Vera** i potvrditi. Kliknuti **Next**. Kliknuti **Yes**.

Pročitati poruku vezanu uz pomicanje miša. Kliknuti na **Format**. Kliknuti **Exit**.

d) Kreirana je nova particija i treba joj omogućiti pristup.

Odabrati slovo **V:** pod kojim će se pristupiti particiji. Kliknuti **Mount** i pročitati poruku.

Pozicionirati se u:

Volumes->Select File

Odabrati datoteku **Vera** u direktoriju **SIS_LV01** i kliknuti **Open**.

Kliknuti na **Mount** i unijeti traženu lozinku **Vera**.

Što se u glavnom prozoru **VeraCrypt-a** pojavilo kod **V:** particije?

e) **U File exploreru** pogledati da li je omogućen pristup particiji **V:**.

Na particiji **V:** kreirati tekstualnu datoteku **lozinke.txt** i u nju unijeti proizvoljni tekst.

f) Vratiti se u **VeraCrypt** aplikaciju i kliknuti **Dismount**.

U **Start->Computer** pogledati da li je još uvijek omogućen pristup particiji **V:**?

Što se dogodilo?

Mogu li ostali korisnici pristupiti particiji **V:** i datoteci **lozinke.txt**? Odgovoriti u bilježnicu.

Zadatak 7: Zadatak za ocjenu

a) Ulogirati se kao korisnik koji ima **administratorske** ovlasti.

b) Unutar direktorija **SIS_LV01** kreirati poddirektorij pod imenom **CYPHER** i ako treba postaviti sva prava za sve korisnike **TEST1, TEST2 i TEST3**.

c) Kao korisnik **TEST1**, unutar direktorija **CYPHER** kreirati poddirektorij **C1** i u njemu tekstualnu datoteku **t1**.

d) Kao korisnik **TEST2**, unutar direktorija **CYPHER** kreirati poddirektorij **C2** i u njemu tekstualnu datoteku **t2**.

e) Kao korisnik **TEST3**, unutar direktorija **CYPHER** kreirati poddirektorij **C3** i u njemu tekstualnu datoteku **t3**.

f) Kao korisnik **TEST1** postavite enkripciju na datoteku **t1** i mogućnost pristupa toj datoteci dodajte i korisniku **TEST2**.

g) Kao korisnik **TEST2** postavite enkripciju na datoteku **t2**.

h) Kao korisnik **TEST3** postavite enkripciju na datoteku **t3** i mogućnost pristupa toj datoteci dodajte i ostalim korisnicima **TEST1** i **TEST2**.

i) Aplikacijom **VeraCrypt** enkriptirajte cijeli direktorij **CYPHER**.

Provjera znanja:

1) Pokazati da li su korisniku TEST3 dodijeljeni neki certifikati. (1 bod)
2) Pokazati kako se enkriptira direktorij. (1 bod)
3) Kako se kreira certifikat za korisnika? (1 bod)
4) Zašto se radi pohrana certifikata i ključeva? (1 bod)
5) Koja ja veza ključeva i korisničke lozinke? (1 bod)
6) Čemu služi VeraCrypt aplikacija? (1 bod)

Ocjene: 6 bodova = 5 ; 5 bodova = 4 ; 4 boda = 3 ; 3 boda = 2 ; <3 boda = 1