# Zaštita pristupa datotekama, direktorijima i diskovima metodom enkripcije

## Teorijski uvod

Enkripcija je proces pretvaranja podataka u oblik koji je nečitljiv bez odgovarajućeg ključa. Koristi se za zaštitu povjerljivih informacija od neovlaštenog pristupa. Postoje dvije osnovne vrste enkripcije:  
- Simetrična enkripcija: koristi isti ključ za enkripciju i dekripciju podataka.  
- Asimetrična enkripcija: koristi par ključeva – javni ključ za enkripciju i privatni ključ za dekripciju.  
  
Zaštita pristupa datotekama, direktorijima i diskovima enkripcijom osigurava da samo ovlašteni korisnici mogu pristupiti osjetljivim podacima, što je ključno u poslovnom i osobnom okruženju.

## Zadaci i rješenja za Windows OS

### 1. Enkripcija datoteka pomoću EFS (Encrypting File System)

Zadatak: Enkriptiraj tekstualnu datoteku pomoću EFS-a.  
Rješenje:  
1. Desni klik na datoteku → Properties → Advanced.  
2. Označi “Encrypt contents to secure data”.  
3. Klikni OK i Apply.  
4. Datoteka će biti označena zelenom bojom.

### 2. Enkripcija diska pomoću BitLocker-a

Zadatak: Enkriptiraj USB stick pomoću BitLocker-a.  
Rješenje:  
1. Otvori Control Panel → BitLocker Drive Encryption.  
2. Odaberi USB disk i klikni “Turn on BitLocker”.  
3. Odaberi način otključavanja (lozinka, USB ključ).  
4. Spremi recovery key na sigurno mjesto.

### 3. Enkripcija pomoću VeraCrypt-a

Zadatak: Kreiraj enkriptirani kontejner pomoću VeraCrypt-a.  
Rješenje:  
1. Pokreni VeraCrypt i klikni na 'Create Volume'.  
2. Odaberi 'Create an encrypted file container'.  
3. Slijedi korake za odabir lokacije, veličine, algoritma i lozinke.  
4. Montiraj kontejner kao virtualni disk.

### 4. Enkripcija pomoću PowerShell-a

Zadatak: Automatiziraj enkripciju datoteka pomoću PowerShell skripte.  
Rješenje:  
Primjer naredbe:  
cipher /e "C:\Users\Korisnik\Documents\osjetljiva\_datoteka.txt"

## Zadaci i rješenja za Linux OS

### 1. Enkripcija datoteka pomoću gpg

Zadatak: Enkriptiraj datoteku pomoću GnuPG.  
Rješenje:  
1. Enkriptiraj:  
gpg -c tajna.txt  
2. Unesi lozinku.  
3. Dekriptiraj:  
gpg tajna.txt.gpg

### 2. Enkripcija direktorija pomoću ecryptfs

Zadatak: Osiguraj direktorij s automatskom enkripcijom.  
Rješenje:  
1. Instaliraj ecryptfs-utils.  
2. Montiraj direktorij:  
sudo mount -t ecryptfs /home/user/secure /home/user/secure

### 3. Enkripcija diska pomoću LUKS i cryptsetup

Zadatak: Enkriptiraj particiju pomoću LUKS-a.  
Rješenje:  
1. Instaliraj cryptsetup.  
2. Enkriptiraj:  
sudo cryptsetup luksFormat /dev/sdX  
3. Otvori disk:  
sudo cryptsetup luksOpen /dev/sdX secure\_disk

### 4. Automatizacija enkripcije skriptama

Zadatak: Napravi bash skriptu koja enkriptira sve .txt datoteke u direktoriju.  
Rješenje:  
Primjer skripte:  
#!/bin/bash  
for file in \*.txt; do  
 gpg -c "$file"  
done