DataHeaven – Dokumentacija projekta

# 1. Opis projekta

DataHeaven je Java desktop aplikacija razvijena korišćenjem Swing biblioteke. Omogućava korisnicima sigurno upravljanje fajlovima korišćenjem AES enkripcije. Podaci se čuvaju lokalno, a ime fajlova i njihovi sadržaji su šifrovani.

# 2. Tehnologije

* Java SE (Swing GUI)
* AES-GCM i AES-CBC enkripcija
* SHA-256 heširanje
* Swing GUI (CardLayout, JTable, JTree)

# 3. Struktura projekta

Projekat koristi sledeće klase u okviru paketa 'dataheaven':

* DataHeaven.java – glavna aplikacija i GUI okruženje.
* LoginPanel.java – panel za prijavu korisnika.
* RegisterPanel.java – panel za registraciju.
* UserServices.java – pomoćne metode za korisnike (provera, registracija, hash funkcija).
* FilePanel.java – upravljanje fajlovima i folderima sa GUI prikazom i enkripcijom.
* NodeInfo.java – pomoćna klasa za prikaz informacija u JTree.
* GlowBorder.java – vizuelna obrada unosa sa greškom.

# 4. Bezbednost i šifrovanje

## 4.1 Enkripcija imena fajlova/foldera

Naziv svakog fajla ili foldera se šifruje pomoću AES algoritma u GCM modu (AES/GCM/NoPadding). Za svaki unos se generiše jedinstveni IV (Initialization Vector) od 16 bajtova. Enkriptovano ime sadrži IV (u hex formatu) + šifrovani deo imena (sadrži ime fajla i IV (u hex formatu)). Kao rezultat toga, ime fajla/foldera na disku izgleda kao heksadecimalni string sa prefiksom '!'.

## 4.2 Enkripcija sadržaja fajlova

Sadržaj fajlova se šifruje korišćenjem AES algoritma u CBC modu (AES/CBC/PKCS5Padding). Za svaki fajl se generiše IV koji se enkodira u Base64 i ugrađuje u ime fajla (u originalnom tekstu pre enkripcije). Upisivanje u fajl se vrši pomoću CipherOutputStream, čime se omogućava enkripcija u toku pisanja.

## 4.3 Dešifrovanje

Dešifrovanje imena fajlova i foldera vrši se korišćenjem istog AES ključa i IV koji se izvlači iz heksadecimalnog naziva fajla. Za sadržaj fajla koristi se AES-CBC, gde se IV dobija iz Base64 enkodovanog dela ugrađenog u originalno ime. Korisnik odabira lokaciju za preuzimanje, a sadržaj se zapisuje u dekriptovanom obliku.

# 5. Validacija korisničkih unosa

Korisnička imena i lozinke se proveravaju pomoću regularnih izraza:

* Korisničko ime: 6–18 karaktera, slova, cifre i specijalni karakteri.
* Lozinka: 8–24 karaktera, bar jedno veliko slovo, broj i specijalan karakter.

# 6. Mogućnosti aplikacije

* Registracija i prijava korisnika
* Dodavanje fajlova i foldera (sa enkripcijom)
* Brisanje fajlova i foldera
* Preuzimanje fajlova (dešifrovano)
* Hijerarhijski prikaz fajlova preko JTree komponente
* Sortiranje i pregled fajlova u tabeli sa metapodacima