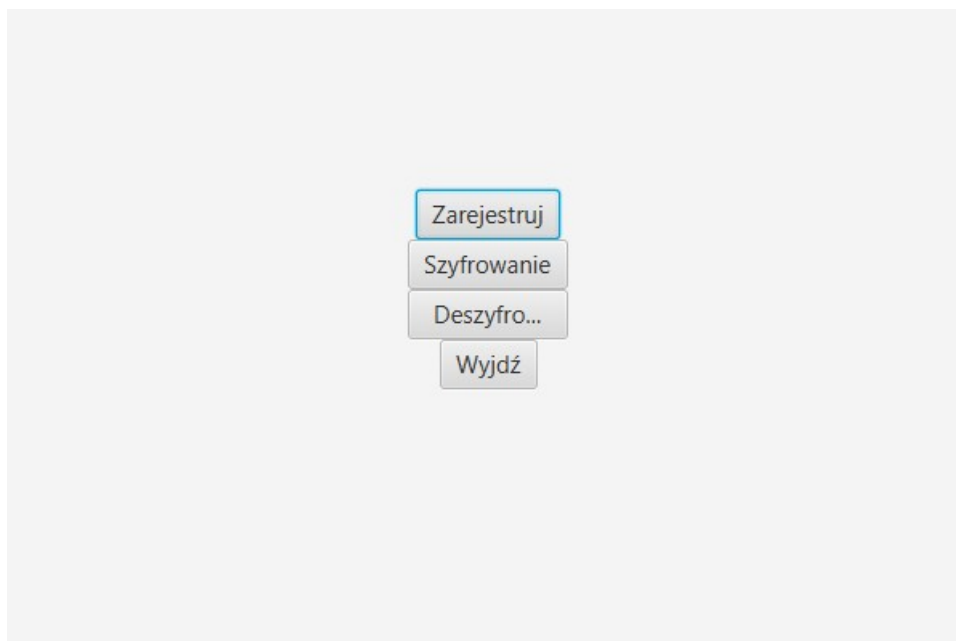


Bezpieczeństwo sieci komputerowych  
**projekt 1 – dokumentacja**

## Interfejs

### 1. Menu główne



Po uruchomieniu aplikacji użytkownikowi wyświetla się menu główne z czterema przyciskami:

- Zarejestruj – przycisk przenosi użytkownika do **widoku rejestracji**
- Szyfrowanie – przycisk przenosi użytkownika do **widoku szyfrowania**
- Deszyfrowanie – przycisk przenosi użytkownika do **widoku deszyfrowania**
- Wyjdź – przycisk służący do zamykania aplikacji

### 2. Widok rejestracji

A registration form with two text input fields. The first field is labeled 'L...' and the second 'H...'. Below the fields are two buttons: 'Rejestruj' and 'Menu główne'.

W tym widoku użytkownik ma możliwość zarejestrowania się w celu późniejszego szyfrowania plików swoim hasłem. W polu tekstowym "Login" podaje nazwę użytkownika, natomiast w polu "Hasło" swoje hasło. Po przyciśnięciu przycisku "Rejestruj" następuje rejestracja użytkownika. Przysisk "Menu główne" służy do powrotu do **Menu głównego**.

### 3. Widok szyfrowania

An encryption interface. At the top left is a button 'Wybierz plik'. Below it is a text input field 'Podaj nazwę nowego p...' containing 'encoded', and a button 'Wybierz folder do z...'. At the top right is a button 'Wybierz tryb szyfrow...' with a dropdown menu showing 'ECB'. Below this is a section 'Użytkownicy' with a list of users: 'Pankiev', 'exampleLogin2', and 'exampleLogin', each with a checked checkbox. At the bottom left is a scrollable area. At the bottom right is a section 'Ogólne informacje:' with the following text: 'Nazwa pliku: Nie wybrano', 'Rozmiar pliku [Mb]: Nie wybrano', 'Rozszerzenie: Nie wybrano', 'Tryb szyfrowania: ECB', and 'Folder zapisu: Nie wybrano'. Below this section are two buttons: 'Szyfruj' and 'Menu główne'.

Ten widok służy do szyfrowania plików. W lewym górnym rogu widnieje przycisk służący do wyboru pliku, który ma być zaszyfrowany. Po jego wciśnięciu otwiera się systemowy dialog do wyboru plików. Poniżej znajduje się pole w którym wpisuje się nazwę pliku wynikowego, natomiast jeszcze niżej przycisk otwierający systemowy dialog do wyboru folderu, w którym będzie znajdować się plik wynikowy. Sekcja "Użytkownicy" służy do wyboru uprzednio zarejestrowanych użytkowników, dla których plik wynikowy ma być możliwy do odszyfrowania. W prawym górnym rogu umieszczona została rozwijana

lista z możliwością wyboru trybu szyfrowania, możliwe opcje to ECB, CBC, CFB lub OFB. W środkowo-dolnej części widoku znajdują się informacje o wybranej konfiguracji oraz rozmiarze wybranego pliku. W prawym dolnym rogu znajduje się przycisk "Szyfruj" uruchamiający szyfrowanie oraz przycisk "Menu główne" przenoszący użytkownika do **Menu głównego.**

### 3. Widok deszyfrowania

Wybierz plik

Podaj nazwę nowego p...

decoded

Wybierz folder do z...

Użytkownicy

Pankiev

Hasło:

...

Ogólne informacje:

Nazwa pliku: Nie wybrano

Rozmiar pliku [Mb]: Nie wybrano

Rozszerzenie: Nie wybrano

Tryb szyfrowania: Nie wybrano

Folder zapisu: Nie wybrano

Deszyfruj

Menu główne

Widok służący do deszyfrowania uprzednio zaszyfrowanych plików. Użytkownik wskazuje lokalizację zaszyfrowanego pliku, wybiera nazwę pliku odszyfrowanego oraz lokalizację w której plik ma być zapisany. Następnie musi znaleźć swoje konto z listy "Użytkownicy" oraz wpisać hasło w celu deszyfrowania. W środkowo-dolnej sekcji wyświetlane są informacje na temat konfiguracji deszyfrowania oraz rozmiar deszyfrowanego pliku. Przycisk "Deszyfruj" odekodowuje plik, a przycisk "Menu główne" powoduje powrót do **Menu głównego.**

### Użyte komponenty

- Oracle JDK 8
- Maven
- Lombok
- JUnit 5
- Google truth

Użyta funkcja skrótu: `sample.ciphering.hashing.SHA256Hasher`

# Testy wydajnościowe

1. Rozmiar pliku: 550Mb

Tabela z czasami [s]

	ECB	CBC	CFB	OFB
Szyfrowanie	27.007	25.417	25.973	32.215
Deszyfrowanie	31.375	30.281	33.456	32.090

2. Rozmiar pliku: 5Mb

Tabela z czasami [s]

	ECB	CBC	CFB	OFB
Szyfrowanie	0.440	0.454	0.468	0.503
Deszyfrowanie	0.414	0.393	0.419	0.465

## Źródła

<https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html>

<http://edu.pjwstk.edu.pl/wyklady/bsi/scb/index43.html>