**Bezpieczeństwo Systemów Komputerowych**

**Sprawozdanie z zajęć projektowych**

Autorzy:

Dorota Tomczak, 165145

Imię, nazwisko, numer indeksu

Wersja dokumentu: 1.0

**\* \* \* DO USUNIĘCIA \* \* \***

**Wraz z realizacją kolejnych zadań (projektu nr 1 oraz 2) sprawozdanie należy uaktualnić – nie należy tworzyć nowych dokumentów.**

**\* \* \* DO USUNIĘCIA \* \* \***

**Historia zmian**

|  |  |  |
| --- | --- | --- |
| Wersja | Data | Opis zmian |
| 1.0 | 23.04.19 | Utworzenie dokumentu, dodanie źródeł |
| 1.1 | 12.05.19 | Dodanie interfejsów użytkownika, charakterystyki zadania, wyników testów (projekt 1) |

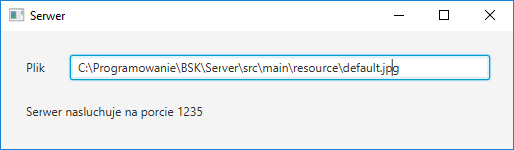
1. **Projekt 1 – Szyfrowanie plików wraz z przekazaniem klucza sesyjnego**
   1. ***Charakterystyka zadania projektowego***

Zadanie projektowe obejmowało utworzenie dwóch aplikacji: serwerowej do szyfrowania plików oraz klienckiej do ich deszyfracji. Wybranym przez nas algorytmem blokowym do realizacji tego zadania jest algorytm Blowfish.

* 1. ***Projekt interfejsów użytkownika***

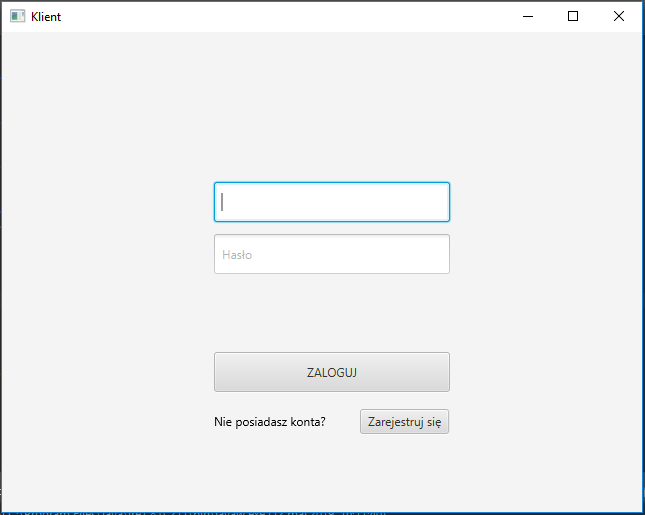
Projekt interfejsów użytkownika wykonano z wykorzystaniem JavaFX oraz narzędzia wspomagającego SceneBuilder.

W aplikacji serwerowej zastosowano jeden ekran, na którym wyświetlane są dwie podstawowe informacje: ścieżka do pliku aktualnie wybranego do szyfrowania oraz informacja w jakim obecnie stanie znajduje się serwer (oczekiwanie na połączenie, szyfrowanie pliku, wysyłanie). Po kliknięciu na pole z nazwą pliku otwiera się menadżer plików, przez który można dokonać zmiany pliku przeznaczonego do szyfrowania.

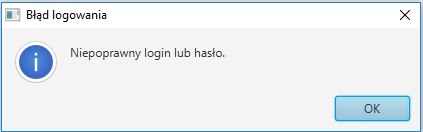


*Okno aplikacji serwerowej*

W aplikacji klienckiej obecne są 4 ekrany: logowania, rejestracji, szyfrowania i deszyfrowania. Ekranem startowym jest ekran przeznaczony do logowania. Po wpisaniu poprawnego loginu i hasła aplikacja przekierowuje do ekranu szyfrowania. W przeciwnym wypadku wyświetla się komunikat o nieprawidłowych danych. Po kliknięciu w przycisk „Zarejestruj się” aplikacja przekierowuje do ekranu rejestracji.

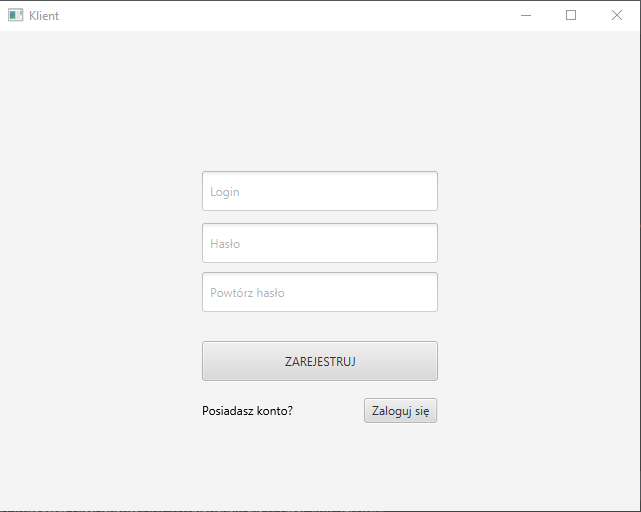


*Ekran logowania aplikacji klienckiej*



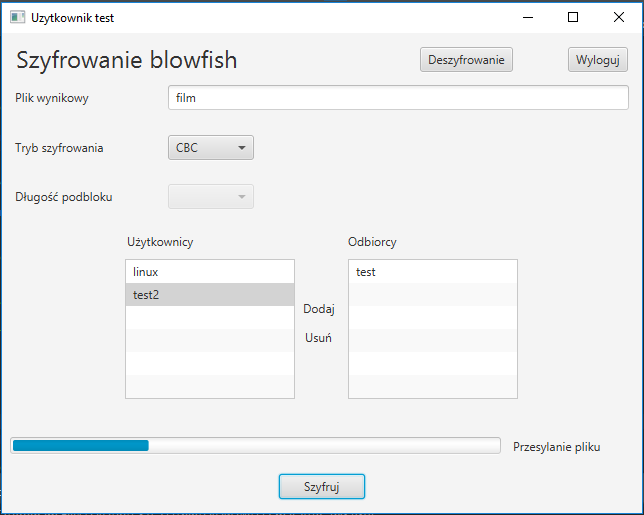
*Komunikat o błędzie logowania*

Na ekranie rejestracji widoczne są 3 pola, które trzeba uzupełnić, aby móc dokonać rejestracji. Pierwsze musi zawierać unikalną nazwę użytkownika, a drugie i trzecie takie same łańcuchy znaków. Po udanej rejestracji aplikacja przekierowuje do ekranu logowania (tak samo po wciśnięciu przycisku „Zaloguj się”). W przypadku nieudanej rejestracji wyświetla się stosowny komunikat.



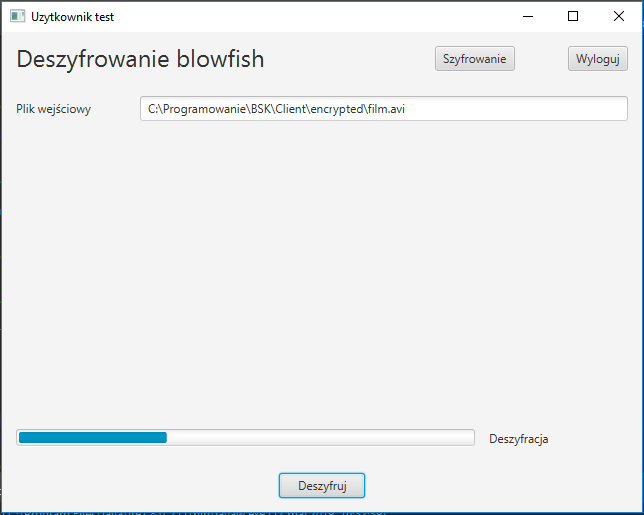
*Ekran rejestracji aplikacji klienckiej*

Ekran szyfrowania umożliwia: wpisanie nazwy, którą będzie miał po odszyfrowaniu odebrany plik; wybranie trybu szyfrowania (ECB, CBC, CFB, OFB) z rozwijanej listy; wybranie długości podbloku dla trybów CFB i OFB z rozwijanej listy (8, 16, 24, 32, 64); wybranie użytkowników, który będą mogli odszyfrować odebrany plik. Pasek postępu umożliwia obserwację postępu przesyłania pliku z aplikacji serwerowej. Szyfrowanie następuje po naciśnięciu przycisku „Szyfruj”. Dwa przyciski w prawym górnym rogu – „Deszyfrowanie” i „Wyloguj” – odpowiadają odpowiednio za: przejście do ekranu deszyfrowania i wylogowania z aplikacji (przejście do ekranu logowania). Nazwa okna aplikacja przedstawia login obecnie zalogowanego użytkownika (tak samo na ekranie deszyfrowania).



*Ekran szyfrowania*

Ekran deszyfrowania umożliwia wybranie pliku przeznaczonego do deszyfracji po naciśnięciu na pole obok etykiety „Plik wejściowy”. Przycisk „Deszyfruj” rozpoczyna deszyfrację. Pasek postępu wskazuje na postęp deszyfracji. Dwa przyciski w prawym górnym rogu – „Szyfrowanie” i „Wyloguj” – odpowiadają odpowiednio za: przejście do ekranu szyfrowania i wylogowania z aplikacji (przejście do ekranu logowania).



*Ekran deszyfrowania*

* 1. ***Opis implementacji zadanej funkcjonalności***

Zawartość podrozdziału

* 1. ***Wyniki przeprowadzonych testów***

Pomiarów dokonano korzystając z metody System.currentTimeMillis() odejmując czas startu od czasu zakończenia.

Plik 737KB

|  |  |  |  |
| --- | --- | --- | --- |
| Tryb | Czas szyfrowania [ms] | Czas przesyłania [ms] | Czas deszyfrowania [ms] |
| ECB | 49 | 838 | 1739 |
| CBC | 46 | 927 | 1616 |
| CFB8 | 130 | 580 | 2792 |
| CFB64 | 34 | 873 | 1917 |
| OFB8 | 159 | 571 | 2379 |
| OFB64 | 45 | 1009 | 2281 |

Plik 14,2 MB

|  |  |  |  |
| --- | --- | --- | --- |
| Tryb | Czas szyfrowania [ms] | Czas przesyłania [ms] | Czas deszyfrowania [ms] |
| ECB | 365 | 20220 | 16670 |
| CBC | 406 | 20234 | 17464 |
| CFB8 | 2055 | 15226 | 25754 |
| CFB64 | 390 | 15020 | 16258 |
| OFB8 | 2143 | 13987 | 27236 |
| OFB64 | 402 | 16469 | 16869 |

Plik 128 MB

|  |  |  |  |
| --- | --- | --- | --- |
| Tryb | Czas szyfrowania [ms] | Czas przesyłania [ms] | Czas deszyfrowania [ms] |
| ECB | 2878 | 128185 | 120490 |
| CBC | 3020 | 127570 | 121343 |
| CFB8 | 18217 | 128101 | 202887 |
| CFB64 | 3378 | 126879 | 122989 |
| OFB8 | 19186 | 123472 | 238570 |
| OFB64 | 3626 | 124191 | 123965 |

* 1. ***Wnioski***

Zawartość podrozdziału

1. **Projekt 2 – Implementacja mechanizmów kontroli dostępu do baz danych**
   1. ***Charakterystyka zadania projektowego***

Zawartość podrozdziału

* 1. ***Projekt struktury bazy danych***

Zawartość podrozdziału

* 1. ***Projekt interfejsu użytkownika***

Zawartość podrozdziału

* 1. ***Wyniki testów***

Zawartość podrozdziału

* 1. ***Wnioski***

Zawartość podrozdziału

1. **Literatura**

[1] Artykuł.

[2] Strona internetowa, (data dostępu).

[3] Książka.

[1] <https://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html>, (02.03.19).

[2] <https://docs.oracle.com/cd/B14099_19/idmanage.1012/b15565/oracle/security/crypto/core/Blowfish.html>, (02.03.19).