Bezpieczeństwo Systemów
i
Usług Informatycznych
Bezpieczny komunikator

Rafał Pieniążek

prowadzący : mgr inż.Przemysław Świercz

1 Cel i zakres projektu

Celem projektu było zaimplementowanie bezpiecznego komunikatora. Do wymiany kluczy szyfrujących wykorzystano algorytm Diffiego-Hellmana. Aplikacja pozwala na ustalenie wspólnego klucza szyfrującego poprzez wymianę kilku informacji niezbędnych do obliczenia bezpiecznego wyniku. Aplikacja umożliwia ponadto zaszyfrowanie i odszyfrowanie wiadomości poprzez szyfr Cezara i Xorowanie wiadomości kluczem. Algorytm szyfrowania Cezara został przetestowany jednostkowo dzięki bibliotece JUnit.

2 Sposób wykonania projektu

Projekt został wykonany w języku Java, przy pomocy biblioteki umożliwiającej nawiązywanie połączenia poprzez Sockety webowe. Aplikacja wspiera uzgodniony podczas zajęć format wymiany informacji typu JSON. Kolejne typy wiadomości są rozpoznawane i przetwarzane przy wsparciu biblioteki Gson.

2.1 Generowanie kluczy

Dwie długie liczby pierwsze zostają wygenerowane losowo dzięki wsparciu wbudowanej biblioteki Javy - BigInteger. Znajdująca się tam metoda possiblePrime() spełnia wymagania tego projektu. Dla każdego nowego klienta generowane są nowe liczy p i g, co pociąga za sobą różne liczy A i B, oraz secret.

2.2 Kodowanie wiadomości

Zaimplementowano dwa rodzaje szyfrowania - szyfr Cezara z przesunięciem secret modulo 26, oraz xorowanie kolejnych bitów wiadomości z bitami secretu.

2.3 Architektura projektu

Podczas rozowoju projektu dbano o czystość kodu, oraz starano się wykorzystać w jak najlepszym stopniu wzorce projektowe. Zarówno w implementacji serwera,

jak i Klienta znaleźć można wzorzec Polecenie.Pozwolił on odseparować pewien model wynikający z założeń projektu, od logiki operującej na niej. Dodatkowo wykorzystano wzorzec Fabryki do tworzenia modułu szyfrującego wiadomości.

3 Wnioski

Wykonanie projektu umożliwiło stworzenie dobrej i bezpiecznej architektury aplikacji typu klient - serwer. Dodatkowo samodzielne zaimplementowanie algorytmu pozwoliło lepsze zrozumienie zależności występujących pomiędzy kolejnymi krokami algorytmu.