1 Cel zadania

Celem zadania była implementacja komunikatora sieciowego wspierającego wymianę kluczy przy pomocy protokółu Diffiego-Hellmana. Ponadto należało wykorzystać wymienione klucze do szyfrowania wiadomości przy pomocy szyfru Cezara, funkcji XOR lub brak szyfrowania. Wszystkie wiadomości miały być przesyłane w formacie JSON oraz przekodowane przy pomocy kodowania transportowego Base64.

2 Sposób wykonania zadania

Komunikator został stworzony w języku Java 8 ze względu na: wieloplaftofomowść, możliwość programowania sieciowego (sockety). W projekcie użyto wspomagajacych bibliotek takich jak: Lombok (generowanie getterów i setterów), Jackson (praca z formatem JSON), Apache-Commons (praca ze Stringami) oraz JUnit (testy jednostkowe) Klient jak i Serwer uruchamiają dwa wątki, jeden odpowiedzialny za nasłuchiwanie (ListenerThread), a drugi (SenderThread) za wysyłanie tego co wpisał użytkownik. Przy autoryzacji użyto klas CallableFuture z nowego API java.util.concurrent, co pozwala na wymianę kluczy w dowolnej kolejności. Do kodowania Base64 wykorzystano klasę z pakietu java.util.Base64 dostępnego od wersji 1.8 języka Java. W projekcie wykorzystano wzorce projektowe co powinno pozytywnie wpłynąć na czytelność kodu.

- Fabryka (EncryptionFactory) - tworzenie obiektu odpowiedzialnego za szyfrowanie.
- Strategia (Operation) - wykorzystano przy przetwarzaniu znaków w Szyfrze Cezara.
- Obserwator - implementacja obserwatora pozwoli na rozszerzanie komunikatora o dodatkowe filtry przy przy wyświetlaniu wiadomości (np.: ukrywanie nieodpowiednich słów).
- Fasada - (TalkFacade) uproszczenie uruchomienie całego systemu rozpoczęcia konweracji.

Liczby generowane są przy użyciu metody probalbyPrime() z klasy BigInteger. W projekcie stworzono przykładowy filtr wiadomości, który zamienia słowo 'test' na '****'. Napisane zostały testy jednostkowe testujące szyfr Cezara, funkcję XOR oraz wyliczanie kluczy wykorzystywanych w protokole Diffiego-Hellmana.

3 Wnioski

Samodzielna implementacja protokołu Diffiego-Hellmana pozwoliła lepiej zrozumieć schemat działania i uzgadniania kluczy oraz zwróciła uwagę na ważny temat jakim jest bezpieczeństwo aplikacji sieciowych.