Wrocław, 26/10/2020 r.

Dominik Kinastowski
Indeks 242081

Raport: Komunikator z szyfrowaniem

1. Cel zadania.

Zadanie polegało na zaimplementowaniu czatu pozwalającego na zabezpieczoną (szyfrowaną) sekretnym kluczem komunikację. Klucz należało uzgodnić protokołem Diffiego-Hellmana.

2. Wykonanie zadania

Zadanie zostało wykonane w sposób przyrostowy opisując kolejne zmiany opisami dokonywanych commitów. Skrócona chronologiczna reprezentacja zmian:
- pierwsze przesłanie wiadomości
- zmiana formatu wysyłanej wiadomości na json
- podtrzymanie komunikacji (więcej niż jedna wiadomość)
- akceptowanie wielu klientów przez serwer
- utworzenie enkryptora (klasy szyfrującej tekst wiadomości)
- zaimplementowanie protokołu Diffiego-Hellmana
- zaszyfrowanie wiadomości ustalonym kluczem
- dodanie kodowania base64

Serwer obsługuje wielu klientów jednocześnie, jednak dla użytkownika trudno rozróżnić od kogo przychodzi wiadomość I do kogo jest wysyłana. Sensownym rozwiązaniem tego problemu byłoby zaimplementowanie prostego interfejsu graficznego (oddzielne okno dla każdej konwersacji), na który zabrakło mi czasu. Zaimplementowany protokół Diffiego-Hellmana funkcjonuje na zahardcodowanych wartościach. Minusem jest też komunikacja, która działa jednostronnie – możliwe jest wysłanie tylko pojedynczych wiadomości, muszą być wysyłane naprzemiennie.

3. Wybrana technologia

Do zaimplementowania rozwiązania wybrana została java wersja 15, z uwagi na podobieństwo do jednego z zadań wykonywanych w zeszłym semestrze (komunikator SOAP-owy). Dodatkowym plusem jednorodnej technologii wykorzystywanej do napisania zarówno klienta jak I serwera było de facto pisanie tylko jednego klienta komunikatora, który został użyty również w implementacji serwera.

4. Wnioski

Protokół Diffiego-Hellmana, przynajmniej w podstawowej wersji jest bardzo łatwy do zaimplementowania.