Bezp. syst. i usług inform. 2

Komunikator z szyfrowaniem, protokół Diffiego-Hellmana

Marcel Kończyk, 210060

1. Cel Projektu

Celem projektu jest napisanie aplikacji, komunikatora wykorzystującego protokół Diffiego-Hellmana oraz podstawowe szyfrowania takie jak: Szyfr Cezara oraz jednobajtowy xor.

2. Sposób wykonania zadania

Zadanie zostało wykonane zgodnie ze schematem przekazanym przez prowadzącego na zajęciach (Rys 1).

Stage	A (client)	B (server)
1	{ “request”: “keys” } →	
2		← { “p”: 123, “g”: 123 }
3	{ “a”: 123 } →	← { “b”: 123 }
4	{ “encryption”: “none” } →	
5	{ “msg”: “...”, “from”: “John” } →	← { “msg”: “...”, “from”: “Anna” }

Rys 1. Przebieg komunikacji

1. Po połączeniu do serwera klient prosi o liczby p oraz g.
2. Serwer wysyła do klienta liczby p oraz g.
3. Serwer i klient wymieniają się publicznymi wartościami A oraz B:
    a. Klient wysyła do serwera obliczoną wartość A.
    b. Serwer wysyła do klient obliczoną wartość B.
    UWAGA: a) oraz b) mogą nastąpić w dowolnej kolejności
4. [OPCJONALNIE] Klient wysyła do serwera informację o żądanym sposobie szyfrowania wiadomości.
    UWAGA: Krok ten jest opcjonalny. Jeżeli klient nie wyśle tej informacji, to strony przyjmują domyśle szyfrowanie ustawione na “none”.
5. Klient oraz serwer wymieniają się szyfrowanymi wiadomościami.

Wiadomości powinny być szyfrowane za pomocą szyfru:

- none (domyślny)
- szyfr cezara
- xor jednobajtowy

kolejno zakodowane przy pomocy kodowania Base64 I wysłane do serwera/clienta, po czym serwer/client powinnien odszyfrować znając klucz szyfrowania.

3. Implementacja

Projekt został zaimplementowany w języku Java SE 1.8, korzystając z narzędnia do budowania projektu Maven oraz pluginu do formatowania JSONów o nazwie GSON. Projekt napisany został przy użyciu środowiska Intelij IDEA Ultimate 2016.

4. Wnioski

Największą trudność sprawiło szyfrowanie metodą xor jednobajtowy, komunikacja używając tego szyfrowania może nie do końca działać tak jak powinna. Wbudowane biblioteki w Javie ułatwiły implementacje niektórych części aplikacji, np. Szyfrowanie przy pomocy Base64.

5. Podsumowanie

W projekcie zrealizowane zostało:

- Implementacja protokołu Diffiego-Hellmana
- Metody szyfrowania takie jak szyfr cezara czy xor jednobajtowy
- Komunikacja multi klient – serwer
- Komunikacja za pomocą formatu JSON

Aplikacja miała za zadanie pokazania samej komunikacji, co zostało zrealizowane. Nie został zaimplementowany żaden interfejs graficzny.