Marcin Bukowiecki 209799

grupa: środa 15:15

Zadanie:

Należy przygotować komunikator (chat) klient-serwer wspierający bezpieczną wymianę sekretu (protokół Diffie-Hellman) oraz obsługujący zadany format komunikacji.

1. Po połączeniu do serwera klient dostaje liczby p oraz g.

2. Serwer wysyła do klienta liczby p oraz g.

3. Serwer i klient wymieniają się publicznymi wartościami A oraz B:

4. Klient wysyła do serwera obliczoną wartość A.

5. Serwer wysyła do klient obliczoną wartość B.

6. Klient oraz serwer wymieniają się szyfrowanymi wiadomościami (szyfr Cezara).

Testy zostały wykonane dla poszczególnych klas i zweryfikowane poprawnosc działania szyfru Cezara, protokołu oraz wyliczanie liczb pierwszych.

Aplikacje udało się wykonać w fazie prototypowej, czyli komunikaty wiadomości sa z góry ustalone. Aplikacja przekazuje zaszyfrowane komunikaty szyfrem cezara.

Największy problem sprawiło przekazywanie wiadomości odpowiednio zaszyfrowane oraz dostosować połączenie protokołem Diffiego-Hellmana.

Aplikacje można rozbudować o dodatkow czytane komunikaty z pliku bądź też wprowadzanie ręcznie do aplikacji.