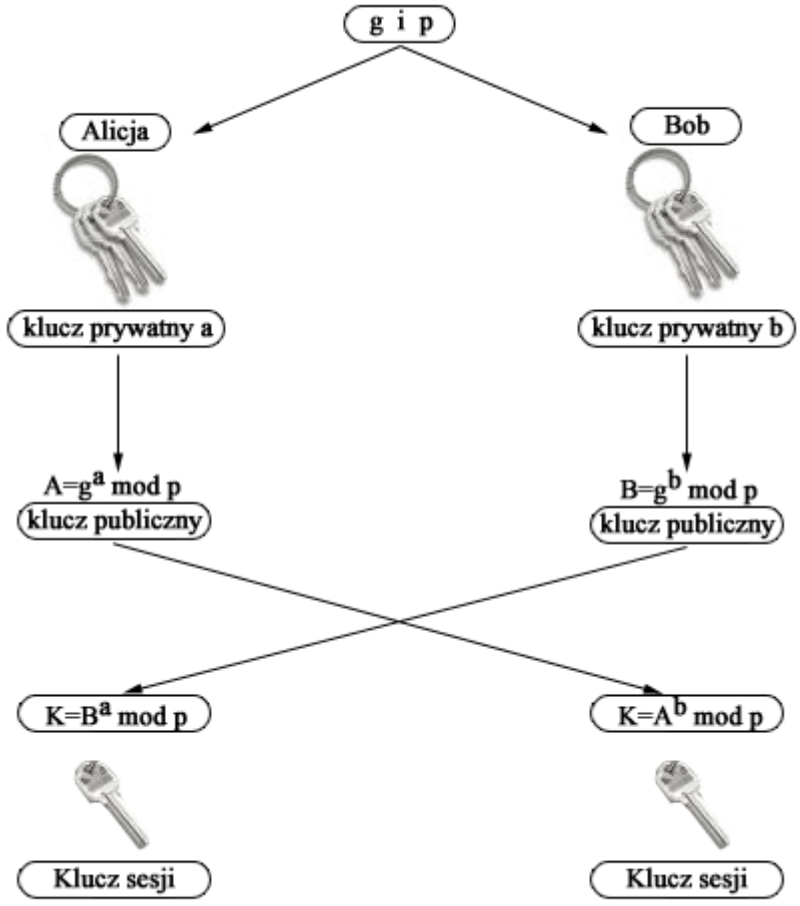
Raport - Komunikator z szyfrowaniem

1. Cel zadania
   Stworzenie komunikatora (chatu) klient-serwer wspierającego bezpieczną wymianę sekretu (protokół Diffie-Hellman) oraz obsługującego format danych JSON.

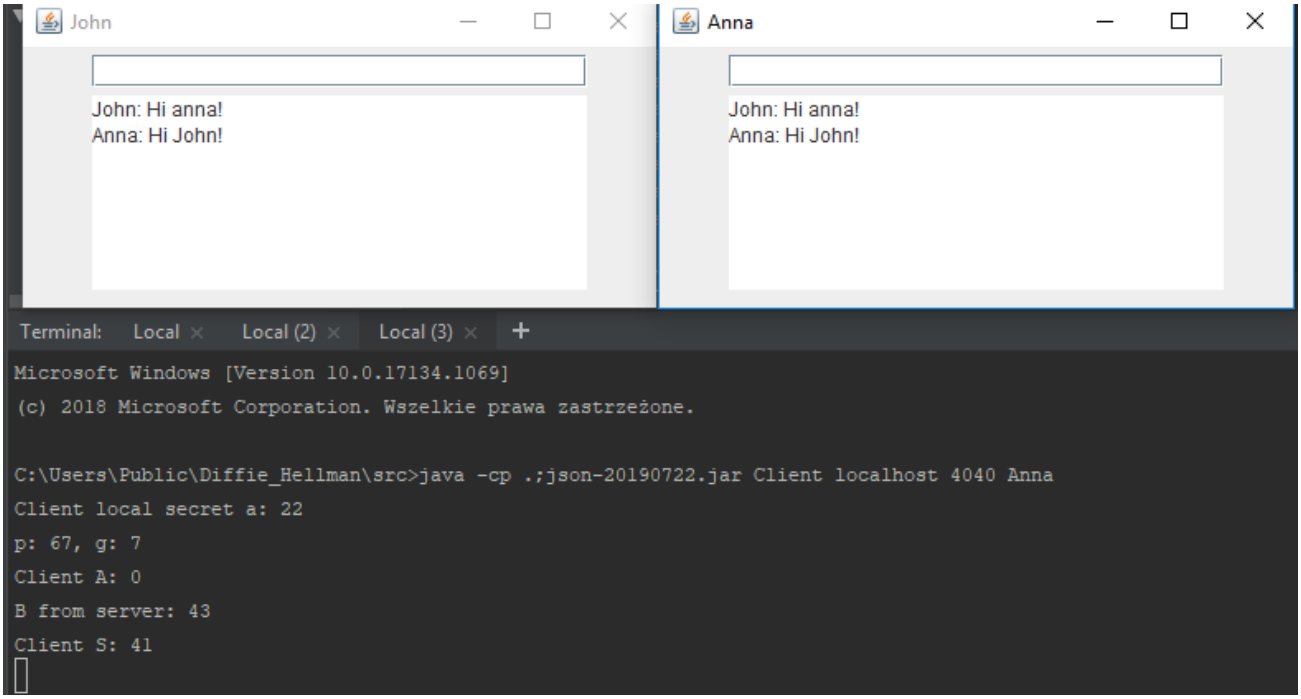
2. Protokół Diffie-Hellman

   Protokół uzgadniania kluczy Diffie-Hellman jest wykorzystywany w kryptografii do ustalenia jednego klucza dla obu stron transakcji bez przesyłania żadnych poufnych informacji. Tak wygenerowany klucz jest później wykorzystywany przez algorytm symetryczny do szyfrowania połączenia między odbiorcą, a nadawcą. Dzięki temu można zabezpieczyć transakcję przed podsłuchiwaniem przez osoby postronne.



3. Sposób wykonania
   - Komunikator działa w architekturze client-server, z możliwością obsługi wielu klientów (klienci zaimplementowani jako lista socketów).

- Obsługa formatu JSON
- Kodowanie i dekodowanie wiadomości z wykorzystaniem base64
- Serwer oraz klient mają te same klucze publiczne p oraz g, i są one zdefiniowane w kodzie. Klucz prywatny serwera również jest stały, natomiast klucz prywatny klienta jest wartością losową z przedziału <1,27>. Rozwiązanie to może nie jest najbardziej optymalne, jednak zostało najlepiej opisane w literaturze
- Wiadomości zostają przesyłane do wszystkich użytkowników
- Na ten moment brakuje szyfrowania xor oraz cezara
- Komunikator został napisany jako prosta aplikacja okienkowa z wykorzystaniem bibliotek AWT i swing



Rys.1 Przykład działania aplikacji.

4. Użyte techlogie

- Aplikacja została napisana w języku JAVA, ponieważ w tej technologii mam największe doświadczenie.