Podstawy Ochrony Danych – laboratorium AGC
D-H - Implementacja algorytmu Diffiego-Hellmana uzgadniania klucza sesyjnego

Cel ćwiczenia laboratoryjnego: zapoznanie się z algorytmem Diffiego-Helmana – asymetrycznym algorytmem uzgadniania klucza sesyjnego oraz analiza możliwego ataku na ten algorytm.
Materiały do laboratorium: materiały z wykładu oraz materiały dodatkowe podane przez prowadzącego.

Zadanie:

Algorytm Diffiego-Helmana oparty jest na trudności obliczania logarytmów dyskretnych w ciałach skończonych. Wykorzystywany jest do dystrybucji kluczy (nie do szyfrowania i deszyfrowania.

Algorytm:

1. A i B uzgadniają ze sobą w sposób jawny wybór dwóch dużych liczb całkowitych **n** – duża liczba pierwsza i **g** – pierwiastek pierwotny modulo n, i gdzie 1<g<n.
2. A wybiera losową dużą liczbę całkowitą x (tajną) – to będzie jej klucz prywatny i oblicza $X=g^x \bmod n$
3. B wybiera losową dużą liczbę całkowitą y (tajną) – to będzie klucz prywatny osoby B i oblicza $Y=g^y \bmod n$
4. A i B przesyłają do siebie nawzajem obliczone X i Y.
5. A oblicza $k= Y^x \bmod n$
6. B oblicza $k= X^y \bmod n$
7. Mogą teraz używać k jako klucza sesji (np. do algorytmu blokowego).

Zadaniem jest implementacja algorytmu D-H. Algorytm ten można łatwo rozszerzyć na grupę użytkowników (dla chętnych implementacja algorytmu dla grupy)

Sprawozdanie:

1. Screenshot z aplikacji.
2. Przeanalizuj, czy są jakieś ograniczenia dla użytych parametrów?
3. Jakie dane można podsłuchać i czy możesz zaproponować jakiś schemat ataku?
4. Dodatkowe wnioski.