Cel ćwiczenia laboratoryjnego: Poznanie metod szyfrowania wykorzystujących schematy progowe.

Zadanie ze współdzielenia sekretów – z wykorzystaniem metody Shamira

Schematy współdzielenia sekretów są wielostronnymi protokołami związanymi z ustanawianiem kluczy. Problem polega na tym, że klucz/sekret dzieli się na części zwane udziałami i następnie rozsyła pomiędzy użytkowników. Aby odzyskać, zrekonstruować pierwotny sekret wymagana jest określona liczba udziałów (określony podzbiór udziałów zwany progiem).

Zadanie 2:

Zaimplementuj aplikację, która pozwala na odtworzenie sekretu zgodnie ze schematem Shamira. Narzędzie powinno wizualizować poszczególne etapy działania algorytmu oraz pozwalać na modyfikację parametrów takich jak:

- Całkowita liczba udziałów,
- Wymagana liczba udziałów do odtworzenia sekretu
- Sekret
- Liczba pierwsza