POD – instrukcja do zajęć laboratoryjnych
Metody podziału sekretu

Ćwiczenie nr 6

Definicje

- n – liczba wszystkich udziałów,
- t – liczba udziałów wymaganych do odtworzenia sekretu.

Trywialna metoda dzielenia sekretu (t, n) [t = n]

- k – wartość liczbowa określająca rozmiar przestrzeni liczbowej,
- s – sekret reprezentowany za pomocą liczby całkowitej z zakresu *0* do *k-1*.

Faza podziału sekretu

1. Wyznacz w sposób losowy *n-1* wartości należących do zbioru <*0*; *k-1*>.
2. Wyznacz *n*-ty udział:

$$s_n = (s - s_1 - s_2 - \cdots - s_{n-1}) \bmod k \tag{1.1}$$

3. Przekaż uzyskane udziały do odbiorców.

Faza odtwarzanie sekretu

1. Zbierz *n* udziałów.
2. Zsumuj wszystkie wartości oraz wykonaj operację modulo *k*:

$$s = (s_1 + s_2 + \cdots + s_n) \bmod k \tag{1.2}$$

3. Uzyskana wartość stanowi sekret.

Schemat Shamira (t, n) [t <= n]

- s – sekret reprezentowany za pomocą liczby całkowitej z zakresu *0* do *p-1*,
- a_0 – wyraz wolny wielomianu; wartość sekretu.

Faza podziału sekretu

1. Wygeneruj dużą, losową liczbę pierwszą p taką, że $p > s$ i $p > n$.
2. Wyznacz w sposób losowy *t-1* liczb $a_1, a_2, \ldots, a_{t-1}$.
3. Dla każdego udziału s_i wyznacz:

$$s_i = s + \sum_{j=1}^{t-1} a_j x^j \mod p \tag{1.3}$$

4. Pojedynczy udział jest reprezentowany jako para liczb postaci:

$$(i, s_i)$$

5. Przekaż uzyskane udziały do odbiorców.

Faza odtwarzania sekretu

1. Zbierz t udziałów.
2. Wyznacz wartość wyrazu wolnego przy użyciu wielomianu interpolacyjnego Lagrange'a:

$$f(x) = \sum_{i=1}^{t} s_i \left(\prod_{j=1, i \neq j}^{t} \frac{x - x_j}{x_i - x_j} \mod p \right) \tag{1.4}$$

3. Uzyskana wartość stanowi sekret.

Zadania szczegółowe

1. Zaimplementuj aplikację, która pozwala na podział oraz odtworzenie sekretu przy użyciu metody trywialnej. Określ dla jakich wartości metoda ta nie jest bezpieczna. Wskaż podstawowe wady wynikające z użycia trywialnego podziału sekretu.
2. Opracuj program umożlwiający podział oraz odtworzenie sekretu zgodnie ze schematem Shamira. Narzędzie powinno wizualizować poszczególne etapy działania algorytmu oraz pozwalać na modyfikację parametrów takich jak:
    a. całkowita liczba udziałów,
    b. wymagana liczba udziałów,
    c. sekret,
    d. liczba pierwsza.

    Jaka jest minimalna, wymagana liczba udziałów, aby algorytm działał poprawnie?
3.* Sporządź sprawozdanie z zajęć. Powinno ono obejmować:
    a. ogólną charakterystykę metod podziału sekretu,
    b. wskazanie i omówienie zalet oraz wad rozwiązań,
    c. omówienie sposobu implementacji,
    d. odpowiedzi na postawione w instrukcji pytania,
    e. zestawienie przykładowych wejść oraz wyjść programów wraz ze stosownymi wnioskami,
    f. krótkie podsumowanie.