Criptografie și securitate CTI

Laborator 12

Sisteme de partajare a secretelor

1. Să se partajaze secretul $S = 13$, pentru o schemă majoritară $k = 3$ din $n = 5$ participanţi, utilizând algoritmul lui Shamir în grupul $(\mathbb{Z}_{17}, \cdot)$ și valorile publice $x_i = i, i = 1, \ldots, 5$ şi valorile aleatoare $a_1 = 10, a_2 = 2$.

2. Să se reconstituie secretul S, din valorile $\{12, 4, 15\}$, știind că acestea au fost obţinute cu ajutorul schemei majoritare $(5, 3)$ a lui Shamir specificată de grupul $(\mathbb{Z}_{17}, \cdot)$ şi valorile publice $\{1, 4, 5\}$.

   Link suplimentar

   `https://en.wikipedia.org/wiki/Shamir%27s_secret_sharing`

   `https://en.wikipedia.org/wiki/Lagrange_polynomial`

3. (a) Folosind schema de partajare a secretelor a lui Goldreich, Ron și Sudan, partajați secretul $S = 789$ folosind numerele $p_1 = 7, p_2 = 11, p_3 = 13, p_4 = 19, p_5 = 23$ și arătați calculând pe hârtie cum utilizatorii 2, 3 și 5 pot reconstrui secretul.

   (b) Ar fi corect să considerăm încă un utilizator pentru care $p_0 = 5$?

   Link suplimentar `https://en.wikipedia.org/wiki/Secret_sharing_using_the_Chinese_remainder_theorem`

4. De ce în problema utilizatorilor "secretoși și zgârciți"

   (a) cei $n - 1$ utilizatori nu pot să determine suma de bani a celui de-al n-lea utilizator decât după ce suma totală este dezvăluită?

   (b) $n - 2$ utilizatori nu pot determina niciodată suma de bani a celorlalți 2 utilizatori.

5. Implementați două din cele 3 scheme de partajare ale secretelor prezentate la curs.