Diszkrét logaritmus

(feladatsor)

Diszkrét modellek alkalmazásai

1. Írjunk függvényt, amely kiszámítja egy adott $\overline{a} \in \mathbb{Z}_p^*$ elem rendjét (ahol p prímszám).

2. Számítsuk ki egy adott $\overline{a} \in \mathbb{Z}_p$-re és $n \in \mathbb{N}$-re az $\overline{a}^n$ hatványt *gyorshatványozással.*

3. Adott p prímszámra keressük meg $\mathbb{Z}_p^*$ összes generátorát.

4. Egy $\overline{g} \in \mathbb{Z}_p^*$ generátorra számítsuk ki egy adott $\overline{a} \in \mathbb{Z}_p^*$ elem $\overline{g}$-alapú diszkrét logaritmusát
   a) egyszerű kereséssel; b) a baby-step giant-step algoritmussal.

5. Szimuláljuk a Diffie–Hellman-kulcscserét, azaz írjunk programot, amely mindkét fél műveleteit végrehajtja, majd kiszámítja a közös titkot mind a két résztvevő módszerével, és ellenőrzi, hogy egyeznek-e. (A p prím és a $\overline{g} \in \mathbb{Z}_p^*$ generátor legyenek állítható paraméterek. Kipróbáláshoz használhatjuk a $p = 23$ és a $\overline{g} = \overline{5}$ értékeket.)

6. Törjük fel a Diffie–Hellman-kulcscserét (ha lehet), azaz írjunk függvényt, amely a kulcscsere nyilvánosan látható paramétereiből diszkrét logaritmussal kiszámítja a közös titkot.