

Polinomok alkalmazásai

(feladatsor)

Diszkrét modellek alkalmazásai

1. Implementáljuk a Lagrange-interpolációt, azaz írjunk függvényt, amely kap $n+1$ helyettesítési értéket egy listában: $[(x_1, y_1), (x_2, y_2), \dots, (x_{n+1}, y_{n+1})]$ (ahol x_i -k mind különbözőek), és kiszámítja azt a legfeljebb n -edfokú polinomot, amelyre $p(x_1) = y_1, p(x_2) = y_2, \dots, p(x_{n+1}) = y_{n+1}$. Ne használjuk a Sage interpolációs függvényét (legfeljebb ellenőrzésre).
2. Szimuláljuk a Shamir-féle titokmegosztást:
 - a) Írjunk függvényt, amely az n, k, S paraméterekből generálja az n résztvevő titokrészeit. Visszatérési érték: (x_i, y_i) pontok n -elemű listája.
 - b) Írjunk függvényt, amely a fenti n részből k -t kap (egy k -elemű listát az (x_i, y_i) pontokkal), és ebből visszaállítja az S titkot.
3. Implementáljuk a CRC-t a következők szerint, a $g = x^4 + x + 1 \in \mathbb{Z}_2[x]$ generátorpolinommal.
 - a) Írjunk függvényt, amely egy adott m üzenetből (ami egy bitsorozat) kiszámítja az elküldött kódszót, azaz m -et kiegészítve a CRC ellenőrző kóddal. Használhatjuk a Sage polinomműveleteit, de a bemenő és a visszatérési érték ne polinom, hanem bitsorozat legyen, azaz 0-k és 1-esek listája.
 - b) Írjunk függvényt, amely a kapott kódszót ellenőrzi, és visszaadja, hogy helyesnek találta-e.
 - c) Generáljunk egy véletlen 16-bites m üzenetet, és próbáljuk ki rajta a)-t, majd a kapott kódszót ellenőrizzük b)-vel.
 - d) Rontsuk el a kapott kódszót, és ellenőrizzük azt is.
 - e) Rontsuk el a kapott kódszót úgy, hogy az ellenőrzésen átmenjen.
4.
 - a) Írjunk függvényt, amely elvégzi az AES *SubBytes* transzformációját egy adott byte-ra. A bemenet és a kimenet egész szám legyen (0 és 255 között).
 - b) Írassuk ki az eredményt mind a 256 lehetőségre egy 16×16 -os táblázatba (sorfolytonosan). Ellenőrizzük az eredményt az Internet segítségével (keressünk rá: "Rijndael S-box").
 - c) Invertálható a transzformáció? (Azaz minden érték pontosan egyszer fordul elő?)
 - d) Van a transzformációnak fixpontja? (Azaz olyan érték, amelynek a képe önmaga?)