

Algoritmuselmélet
Vizsga (minta)

Minden feladat teljes megoldása 10 pontot ér. Az elégségeshez legalább 20 pont elérése szükséges a vizsgán, függetlenül a gyakorlaton szerzett pontszámtól. A feladatokra adott válaszaiban minden állítását indokolja.

1. Az RSA-eljárás (aláírás nélküli változata) folyamán az egyik felhasználó a $p = 5$ és $q = 11$ prímekeket választotta, nyilvános kulcsa $(9, 55)$, titkos kulcsa $(l, 55)$.
 - i, Határozza meg l értékét.
 - ii, Egy másik felhasználó szeretné átküldeni a 2-t titkosított üzenetként a fenti felhasználónak. Mi lesz a titkosított üzenet?
2. Írja le a Miller-Rabin prímtesztet. Mekkora annak a valószínűsége, hogy az eljárás hibázik?
3. Mondja ki a Hilbert Nullstellensatz tételt, majd bizonyítsa a gyenge Nullstellensatz tétel felhasználásával.
4. Adott $G = \{-2x^2 + x^3, -2y + xy, -x^2 + 2y^2\} \subseteq \mathbf{C}[x, y]$ Gröbner-bázis, ahol $x < y$. Legyen $I = (G)$.
 - i, Igaz-e, hogy $x^2 + xy \in I$?
 - ii, Igaz-e, hogy $x^2 + xy \in \sqrt{I}$?
5. Határozza meg $\frac{\sqrt[3]{4} + \sqrt[3]{2} + 1}{2(\sqrt[3]{4} + 1)}$ algebrai szám $\mathbf{Q}$ feletti minimálpolinomját számolás nélkül az $(x^3 - 2, x^2 + x + 1 - y(2x^2 + 1))$ ideál

$$G = \{-1 + 9y - 39y^2 + 33y^3, -16 + 207y - 231y^2 + 17x\}$$

redukált Gröbner-bázisa segítségével, ahol $y < x$.

A kurzus értékelése, ponthatárok:

Feltéve, hogy a vizsgán elért pontszám legalább 20:

2: 40-52

3: 53-64

4: 65-79

5: 80-100