Algebrai és aritmetikai algoritmusok tematika

1. **Prímtesztelés I.**(Véletlent használó módszerek: Fermat, Solovay-Strassen, Miller-Rabin.)
2. **Prímtesztelés II.**(Determinisztikus módszerek: Próbaosztás, AKS algoritmus.)
3. **Nyilvános kulcsú kriptográfia.**(Diffie-Hellman kulcscsere rendszer, RSA, El Gamal kulcsgenerálás, kódolás, dekódolás.)
4. **Faktorizáció.**(Fermat módszere, faktorbázis algoritmus, kvadratikus szita.)
5. **Diszkrét logaritmuskeresés.**(Baby step - Giant step módszer, Index kalkulus algoritmus.)
6. **Elliptikus görbék I.**(Az elliptikus görbe fogalma, csoporttulajdonság, alkalmazás prímtesztelésre.)
7. **Elliptikus görbék II.**(Az elliptikus görbe fogalma, csoporttulajdonság, alkalmazás faktorizációra.)
8. **Polinomfaktorizáció I.**(Négyzetmentes felbontás, különböző fokú felbontás, Cantor-Zassenhaus algoritmus.)
9. **Polinomfaktorizáció II.**(Berlekamp - részalgebra, abszolút Berlekamp - részalgebra, Berlekamp determinisztikus és véltlenített algoritmusa.)
10. **Polinomfaktorizáció III.**(A racionális számtest feletti polinomok felbontására vonatkozó Berlekamp - algoritmus.)
11. **Polinomfaktorizáció IV.**(A Lenstra–Lenstra–Lovász-algoritmus.)
12. **Rácsredukció.**(Rácsok, rövid rácsvektorok, I. Minkowski - tétel, Gauss - algoritmus. Gyenge redukció, Lovász - redukció, a redukált bázis tulajdonságai.)