1. Algebrai struktúrák: csoport, gyűrű, test, véges testek.
2. Műveletek elliptikus görbék pontjaival.
3. Elemi számelméleti ismeretek I: oszthatóság, prímszámok, legnagyobb közös osztó, Euklideszi algoritmus.
4. Elemi számelméleti ismeretek II: kongruencia reláció, műveletek maradékokkal, kis Fermat tétel.
5. Kriptográfiai alapfogalmak, titkosítási rendszerek, támadások, klasszikus titkosító módszerek.
6. Szimmetrikus kulcsú titkosítás – DES.
7. Szimmetrikus kulcsú titkosítás – AES.
8. Blokktitkosítási módok, folyamtitkosítók, otp.
9. Nyilvános kulcsú titkosítás elve, Diffie-Hellman kulcscsere.
10. Az RSA titkosítás és paraméterei.
11. Támadási módszerek az RSA ellen: faktorizáció, gyenge paraméterek, timing attack.
12. Diszkrét logaritmuson alapuló rendszerek, az ElGamal titkosítás.
13. Internet biztonsági protokollok (SSL\TLS) elméleti alapjai, hibrid titkosítás.
14. Kriptográfiai hash függvények és alkalmazásuk a jelszavas azonosításban.
15. Digitális aláírások – RSA aláírás, RSA vak aláírás.
16. Diszkrét logaritmuson alapuló DSA aláírás.
17. Titokmegosztás és titokmegosztási algoritmusok.