1. Szimmetrikus kulcsú rejtjelezés alapelve
2. Aszimmetrikus (nyilvános) kulcsú rejtjelezés alapelve
3. Hozzáférésvédelem feladata
4. Partnerazonosítás feladata
5. Integritásvédelem feladata
6. Kulcsgondozás feladatai
7. Blokk rejtjelezés
8. Kulcsfolyamatos rejtjelezés
9. Lineáris blokk rejtjelező
10. Betű-statisztikai alapú rejtjelfejtés
11. One time pad
12. Tökéletes rejtjelezés
13. Shamir háromlépéses protokollja
14. Egyirányú függvény
15. Helyettesítéses-permutációs rejtjelezés
16. S-box balansz tulajdonság
17. S-box nemlinearitás
18. SPC lavinahatás
19. DES Feistel technika
20. ECB mód blokkséma
21. ECB mód biztonság
22. CBC mód blokkséma
23. CBC mód biztonság
24. CFB mód blokkséma
25. CFB mód biztonság
26. OFB mód blokkséma
27. OFB mód biztonság
28. CTR mód blokkséma
29. CTR mód biztonság
30. Hibasokszorozódás
31. RSA kulcs setup
32. Ismételt négyzetre emelés és szorzás
33. Álprím
34. Fermat primteszt
35. Fermat faktorizáció
36. ElGamal rejtjelező
37. ECDLP
38. ECC DH kulcscsere
39. Digitális aláírás generálása és ellenőrzése
40. Digitális aláírás vs. analóg aláírás
41. Kriptográfiai hash függvény egyirányúsága
42. Kriptográfiai hash függvény ütközésmentesége
43. Születésnapi paradoxonok
44. Születésnapi paradoxon és hash fv. támadása
45. Iterált kriptográfiai hash fv.
46. DM padding
47. Kihívás és válaszvárás a partnerazonosításban
48. Egyirányú függvény és jelszóvédelem
49. Egyszer használatos jelszó
50. Vak aláírás
51. Moduláris négyzetgyökvonás probléma
52. Kerberos blokkvázlat
53. Kerberos ticket
54. Kerberos autheticator