Kriptográfia fogalmak:

1. Támadó modellek (lehallgató, aktív, MIM, dishonest, korrumpáló)
2. Hitelesítés vs. rejtelezés
3. Szimmetrikus kulcsú rejtjelezés alapelve
4. Kerckhoff elv
5. Aszimmetrikus (nyilvános) kulcsú rejtjelezés alapelve
6. Hozzáférésvédelem feladata
7. Partnerazonosítás feladata
8. Integritásvédelem feladata
9. Kulcsgondozás feladatai
10. Blokk rejtjelezés
11. Kulcsfolyamatos rejtjelezés
12. Lineáris blokk rejtjelező
13. Betű-statisztikai alapú rejtjelfejtés
14. One time pad. Tökéletes rejtjelezés
15. Shamir háromlépéses protokollja
16. Egyirányú függvény
17. Helyettesítéses-permutációs rejtjelezés
18. DES Feistel technika
19. ECB mód blokkséma
20. ECB mód biztonság
21. CBC mód blokkséma
22. CBC mód biztonság
23. CFB mód blokkséma
24. CFB mód biztonság
25. OFB mód blokkséma
26. OFB mód biztonság
27. CTR mód blokkséma
28. CTR mód biztonság
29. Hibasokszorozódás
30. RSA kulcs setup
31. RSA biztonsága
32. RSA setup komplexitása. Ismételt négyzetre emelés és szorzás módszere.
33. Fermat álprím fogalma. Fermat primteszt
34. Fermat faktorizáció
35. Kicsi kódoló kulcsok problémája
36. ElGamal rejtjelező
37. Digitális aláírás generálása és ellenőrzése
38. Digitális aláírás biztonsága: existential forgery.
39. Digitális aláírás vs. analóg aláírás
40. Születésnapi paradoxonok
41. Születésnapi paradoxon és hash fv. támadása
42. Iterált kriptográfiai hash fv.
43. Hash fügvények biztonsági követelményei: egyirányúság, ütközésmentesség, második őskép ellenállás, választott kezdőérték melletti támadások
44. DM padding
45. Kihívás és válaszvárás a partnerazonosításban
46. Jelszavas rendszerek alapvető biztonsági problémái
47. Egyirányú függvény és jelszóvédelem
48. Egyszer használatos jelszó
49. Publikus kulcsú rejtjelező algoritmus alapú partnerazonosítás
50. Vak aláírás
51. Moduláris négyzetgyökvonás probléma
52. Fiat-Shamir partnerazonosító protokoll
53. Kerberos access control protokoll . Kerberos ticket. Kerberos autheticator
54. CBC-MAC
55. Existential forgery: CBC-MAC példák
56. Kulcsolt hash (key prefix, key suffix, sandwitch)
57. Kulcsgondozás feladatok.

58. Biztonságos kulcscsere biztonsági szolgáltatásai: implicit kulcshitelesítés, kulcskonfirmáció, explicit kulcshitelesítés, kulcsfrissesség, partnerhitelesítés
59. Needham-Schroeder protokoll és elemzése. Kulcshierarchia.
60. Kerberizált változat.
61. Publikus kulcsú rejtjelező algoritmus alapú kulcscsere protokoll
62. Publikus kulcsú kulcstanusítvány
63. CA fa. Root CA. Tanusítványlánc
64. ISO X.509 tanúsítvány
65. Diffie-Hellmann kulcscsere alap protokol. Passzív és aktív támadó esete.
66. Bit commitment. Távoli pénzfeldobás feladat.
67. Zero knowledge proof (ZKP). Példák: Fiat-Shamir protokoll, ZK cave, ZKP gráf izomorfia problémára.
68. Titokmegosztás feladat. Titokmegosztás Reed-Solomon kód felhasználásával.
69. SSL protokol. Elemei és illeszkedése az Internet protokol architekturába. Record protocol. SSL session. SSL connection. Handshake protocol. Az SSL kulcscsere opciói. Példák: RSA alapú kulcscsere, egyszer használatos DH alapú kulcscsere.
70. IPSEC protocol. AH protokol. ASP protokol. IPSEC üzemmódok (transzport, tunnel). VPN alkalmazás.
71. Elektronikus fizetési rendszerek (EPS). Azonosított, anonim, online, offline EPS. Az ideális EPS tulajdonságai. Digicash protocol. Vak aláírás. Double spending.