Kriptográfia kiskérdések

1. Mivel foglalkozik a kriptográfia?
2. Mi a különbség a kriptográfia és kriptoanalízis között?
3. Mondjon két szteganográfiai módszert!
4. Mik az informatikai biztonság alapvető céljai/szolgáltatásai?
5. Mit jelent a bizalmasság (confidentiality)?
6. Mit jelent a hitelesség (integrity)?
7. Mit jelent a rendelkezésre állás (availability)?
8. Mit jelent a letagadhatatlanság (non-repudiation)?
9. Mondjon három példát a kriptográfia alkalmazási területeire!
10. Mondjon három olyan területet, mely az informatikai biztonság körébe beletartozik a kriptográfiáéba viszont nem!
11. Ismertesse a titkosítás következő alapfogalmait: nyílt szöveg, titkosított szöveg, kulcs, titkosítás, megfejtés, feltörés!
12. Mi az alábbi titkosítási fogalmak angol elnevezése: nyílt szöveg, titkosított szöveg, kulcs, titkosítás, megfejtés, feltörés.
13. Mi az aktív és passzív támadás közti különbség?
14. Ismertesse a szimmetrikus titkosítás modelljét!
15. Ismertesse a nyilvános kulcsú titkosítás modelljét!
16. Mi a legalapvetőbb különbség a nyilvános kulcsú és a szimmetrikus titkosítás között?
17. Miért van szükség nyilvános kulcsú kriptográfiára?
18. Mi a teljes kipróbálás (brute-force)? Mondjon rá példát!
19. Mi a kriptoanalízisen alapuló támadás? Mondjon rá példát!
20. Mik a Kerckhoff követelmények?
21. Mi a Kerckhoff-elv?
22. Mi igazolja a Kerckhoff-elvet?
23. Csoportosítsa a titkosítás elleni támadásokat a támadó rendelkezésére álló információ alapján!
24. Mik a kriptorendszerek értékelési szempontjai?
25. Mi a feltétlen biztonság (unconditional security, perfect security)?
26. Van-e feltörhetetlen titkosítási algoritmus?
27. Mi a kalkuláció biztonság (computational security)?
28. Hogyan növelhető egy megbízható titkosítási algoritmus esetén az általa megvalósított titkosság mértéke?
29. Mi a hamis biztonság csapdája?
30. Mi a különbség az alábbi fogalmak között: feltétlen biztonság – számítási biztonság.
31. Mi a különbség az alábbi fogalmak között: P-doboz (P-box) – S-doboz (S-box)
32. Mi az ismert nyít szöveg alapú támadás?

33. Mi a kriptoanalízis? Mondjon rá egy példát!
34. Definiálja a kriptorendszer fogalmát!
35. Miért kell a kriprorendszer definíciójában az e_K titkosító leképezésnek injektívnek lennie?
36. Definiálja a eltoló (Caesar) titkosítót kriptorendszerként!
37. Definiálja az egyábécés helyettesítés kriptorendszerként!
38. Mekkora a kulcstér mérete egyábécés helyettesítés esetén?
39. Definiálja az affin titkosítót kriptorendszerként!
40. Hogyan alkalmazhatók a nyelvi statisztikák az egyábécés helyettesítés kriptoanalízisében?
41. Mik azok a kriptogrammok?
42. Milyen módszerek léteznek az egyábécés helyettesítsé könnyű feltörhetőségének elkerülésére?
43. Titkosítsa Vigenére-titkosítással az alábbi a ,,TITKOS"nyílt szöveget a "FA" kulccsal. (Ékezetek nélküli 26-betűs angol ábécét használva.)
44. Mi az a Kasiski tesz és mire jó?
45. Hogyan működik a Playfair titkosító?
46. Mit tud mondani a Playfair titkosító kriptoanalíziséről?
47. Hogyan működik a Vernam-titkosító?
48. Mit jelent az, hogy az egyszeri hozzáadásos módszer (OTP) feltétlenül biztonságos?
49. Igaz-e, hogy az egyszeri hozzáadásos módszer (OTP) feltétlenül biztonságos? Válaszát indokolja.
50. Ha az hozzáadásos módszer (OTP) feltétlenül biztonságos, akkor miért nem elterejdt a gyakorlatban?
51. Mi az az Enigma, mi a fő működési elve? Melyik titksosító generációhoz tartozik?
52. Hogyan működnek a produkciós titkosítók?
53. Feistel stuktúrára épül-e a DES? És az AES?
54. Milyen hosszú kulcsot vár a szabványosan megvalósított DES és mennyi ebből az effektív kulcsméret? Hogyan értékelhető ez az algoritmus biztonsága szempontjából?
55. Hogyan szokták megadni a DES S-dobozait? Igaz-e hogy egyetlen DES S-doboz egy 4 bites bemenetbő 6 bites kimenetet készít?
56. Vázolja a DES egy körfüggvényét.
57. Mi az a lavinahatás? Rendelkezik-e vele a DES? És az AES?
58. Mi az a Deep Crack gép? Építettek-e ilyet. Miért?
59. Mi az a 3TDES és hogyan működik?
60. Mi az a 2TDES és hogyan működik?
61. Mi a szerepe nyilvános kulcsú kriptográfiában a nyilvános kulcsnak?
62. Mi a szerepe nyilvános kulcsú kriptográfiában a magánkulcsnak?
63. Miért hívják asszimmetrikusnak is a nyílvános kulcsú kriptográfiát?
64. Mit jelent az, hogy 2048 bites RSA titkosítás. Mi 2048 bit?
65. Milyen alakalmazásai vannak a nyilvános kulcsú kriptográfiának?

66. Miyen függvényeken alapszik a nyilvános kulcsú kriptográfia biztonsága (RSA, Diffie-Hellman)?

67. Mi a véleménye a következő állításról:

    ,,Az RSA biztonságosabb az AES-nél, mert az RSA nyilvános kulcsú, az AES pedig titkos kulcsú módszer."

68. Mi a véleménye a következő állításról:

    ,,A nyilvános kulcsú modern módszerek idővel ki fogják szorítani a szimmetrikus módszereket."

69. Mi a véleménye a következő állításról:

    ,,Az modern szimmetrikus kulcsú titkosítások jóval gyorsabbak a jelenleg ismert nyilvános kulcsú módszereknél."

70. Mi a véleménye a következő állításról:

    ,,Az RSA titkosítás, azért biztonságos, mert nem ismerünk hatékony algoritmust annak eldöntésére, hogy egy szám prím-e vagy sem."

71. Mi a véleménye a következő állításról:

    ,,Egész számok körében a hatványozás nem végezhető el polinom időben, de a moduláris hatványozás igen."

72. Mi a véleménye a következő állításról:

    ,,Az SHA-512 algoritmus meglehetősen lassú, mert minden 1024 bites blokkot 80 körön keresztül dolgoz fel."

73. Mi a véleménye a következő állításról:

    ,,Az Whirlpool modern hash függvény, melyet a TDES algoritmus elvei alapján terveztek."

74. Mi a véleménye a következő állításról:

    ,,Ahhoz, hogy egy hash függvény a HMAC terevezési séma szerint üzenethitelesítő algoritmusként szolgáljon legalább 256 bites hash értéket kell szolgáltatnia."

75. Ismertesse a RSA titkosítás és megfejtés algoritmusát.

76. Ismertesse a RSA kulcsgenerálást.

77. Mik azok az időméréses támadások (timing attack)?

78. Mi az előnyük az elliptikus görbéken alapuló (ECC) tikosítóknak az RSA-val szemben?

79. Milyen blokktitkosító módokat ismer?

80. Mi az ECB mód? Mire alkalmas és mire nem? Miért?

81. Mi a CBC mód? Mik az előnyei?

82. Mi az üzenet helykitöltése (padding)? Miért van rá szükség?

83. Mi a különbség a blokk- és folyamtitkosítók között? Mi a folyamtitkosítók általános működési elve?

84. Mire kell különös figyelmet fordítani a nyilvános kulcsok szétosztása során?

85. Milyen módszerek vannak a nyilvános kulcsok szétosztására? (Elég csak a felsorolás.)

86. Mit jelent a kulcsok nyilvános kihirdetése. Mire használható? Mi a hátránya?

87. Hogyan történik a nyilvános kulcsok szétosztása nyilvános kulcsszolgáltató használata esetén?

88. Mit tartalmaz egy nyilvános kulcs tanúsítvány? Ki állítja ki?

89. Hogyan működik a Diffie-Hellman kulcs-csere és mire jó?

90. Mi a hibrid kulcsszétosztás?

91. Milyen kriptográfiai primitívek használhatók üzenetek hitelesítésére?
92. Mik azok az üzenethitelesítő kódok és hogyan használhatók üzenetek hitelesítésére (titkosítűs nélkül)?
93. Mik azok az hash függvények és hogyan használhatók üzenetek hitelesítésére?
94. Mit jelent egy hash függvény gyenge ütközésmentessége?
95. Mit jelent egy hash függvény erős ütközésmentessége?
96. Ismertesse a születésnap elvű támadást egy h 64 bites hash függvény ellen.
97. Biztonságosabb-e az MD5 hash függvény, mint az SHA-256. Miért?
98. Melyek a digitális aláírás feladatai?
99. Melyek a digitális aláírás tulajdonságai?
100. Mi a DSS?