Kriptográfia próba elővizsga

1. Mi a különbség az alábbi fogalmak között

   a) aktív támadás – passzív támadás

   b) P-doboz (P-box) – S-doboz (S-box)

2. Mi a steganográfia, mi a különbség a kriptográfia és a steganográfia között?

3. Mi az a Kasiski tesz és mire jó?

4. Mit jelent az, hogy az egyszeri hozzáadásos módszer (OTP) feltétlenül biztonságos?

5. Mi a szerepe nyilvános kulcsú kriptográfiában a nyilvános kulcsnak?

6. Mi a véleménye a következő állításról:

   ,,Az RSA titkosítás, azért biztonságos, mert a matematika módszereivel bizonyított, hogy a faktorizáslás nem végezhető el hatékonyan, azaz polinóm időben."

7. Ismertesse a RSA kulcsgenerálást.

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

9. Mik azok az hash függvények és hogyan használhatók üzenetek hitelesítéséra?

10. Mit jelent egy hash függvény erős ütközésmentessége?