Vizsgakérdések

1. Entrópia, zajmentes kódolási tétel, csatornakódolási tétel
2. Korlátok kód méretére
3. Lineáris kód, generátor- és ellenőrző mátrix
4. Igazolja a lineáris kód duálisára vonatkozó fontosabb tulajdonságokat!
5. Mit értünk szindróma dekódoláson?
6. Mi a Hamming-kód? Igazoljuk, hogy perfekt!
7. Mi a Hadamard dekódolás?
8. A ciklikus kód tulajdonságai.
9. Mi a kapcsolat ciklikus kód és duálisa között?
10. Mi az általánosított Reed–Solomon-kód? Mik legfontosabb tulajdonságai?
11. Mit jelent a tökéletes, a szemantikai és a számítási biztonság? Shannon-tétel a tökéletesen biztonságról. Az OTP tökéletes biztonsága.
12. PRG jósolhatósága, biztonságossága, és a belőle képzett folyó titkosítás szemantikai biztonsága.
13. Blokktitkosítás, PRF és PRP (PRF $\rightarrow$ PRG). DES, Feistel-típusú titkosítás. AES. Blokkódolás PRG-ből.
14. Blokktitkosító használatának módjai: ECB, DETCTR, CBC, CBC-tétel, CTR-tétel, összehasonlításuk
15. MAC: CBC-MAC, NMAC (raw-CBC, cascade), PMAC-tétel
16. Hash, ütközésállóság, HMAC, tömörítő függvény
17. Hitelesített titkosítás, CCA
18. Kulcscsere, Merkle Puzzles, Diffie–Hellman protokol, egyirányú kiskapu-függvény (TDF), nyilvános kulcsú titkosítás TDF-ből és annak CCA^{ro}-biztonsága
19. Az RSA titkosítás és biztonsága, Wiener-támadás
20. ElGamal kriptorendszer, az elliptikus görbékre épülő kriptográfia alapjai: pontművelet, diszkrét logaritmus elliptikus görbén.