# Államvizsgatételek az Elektronikus információbiztonság tárgyhoz

1. Mágneses, illetve optikai háttértárakon tárolt adatok védelmi lehetőségei (RAID rendszerek, Keresztcsatolású Reed-Solomon kód, stb.)
2. Számítógépes vírusok fajtái, felismerési, védekezési lehetőségek.
3. Modern szteganográfiai megoldások üzenetek rejtésére (szövegfájl, LSB technika, stb).
4. DES, 3DES kódolás/dekódolás menete, védelmi szintje, alkalmazási területei.
5. AES kódolás menete, védelmi szintje, alkalmazási területei.
6. RSA kódolás menete, védelmi szintje, digitális aláírások.
7. Elliptikus görbék és felhasználási területük.
8. Blokkos rejtjelezés és folyamtitkosítás menete, alkalmazási területei.
9. Hibrid titkosítás, HTTPS, tanúsítványkezelés menete.
10. Titkosított e-mail üzenetváltás lehetőségei, a PGP működési elve, védelmi szintje.
11. Titkosított fájlrendszerek (EFS, BitLocker, FileVault) működése és védelmi szintjük.
12. HASH függvények működése, felhasználási területei.
13. Vezetéknélküli hálózatoknál használatos titkosítási algoritmusok működése, biztonsága (WEP, WPA, WPA2).
14. Webes adatbázisok felépítése, normalizáció. Adatok védelmi lehetőségei. SQL injection, helytelen típuskezelés kihasználása.
15. Keyloggerek típusai, Cross Site Scripting támadási módok.
16. Social Engineering technikák, védekezési lehetőségek.
17. Jelszavak biztonsága, sózás és egyéb biztonságot növelő technikák.
18. Számítógépes hálózat határvédelme: tűzfalak működése, DMZ, PAT, NAT
19. Hálózati forgalom biztonsága, SSH, SSL/TLS, VPN, IPSEC
20. DoS, DDoS támadások és az ellenük való védekezési lehetőségek.
21. Kriptovaluták felhasználási területe, bányászatuk, Darkweb, Deepweb