Kriptográfia tételsor 2007

A vizsgán két tételt kell külön-külön telejsíteni, az első az 1–14. a második a 15–28. tételek közül kerül ki.

1. A kriptográfia fogalma és alapvető feladatai.
2. Titksoítási alapfogalmak, a szimmetrikus és a nyilvános kulcsú titkosítás modellje. Ezen modellek alapvető különbsége.
3. Kriptoanalízis, titkosítás elleni támadások típusai, kriptográfiai rendszerek biztonsága.
4. Caesar-titkosító, eltoló-titkosító, egyábécés helyettesítés és ezen módszerek kriptoanalízise.
5. A Playfair és a Vigenére-titkosító és kriptoanalízisük.
6. A Vernam-titkosító és az egyszeri hozzáadásos módszer (OTP), alkalmazásuk és biztonságuk.
7. Az Enigma működése és kriptoanalízise.
8. Helyettesítő és keverő titkosítók összehasonlítása. Példák keverő titkosítókra. Produkciós titkosítók. Titkosítók generációi.
9. A DES működése.
10. Támadások a DES ellen. A TDES.
11. Az AES és kriptoanalízise.
12. A nyilvános kulcsú kriptográfia alapfogalmai és biztonsága. (Csak általánosan.)
13. Az RSA működése és megvalósítása.
14. RSA kulcsgenerálás. Az RSA biztonsága.
15. Kulcsgondozás.
16. Diffie-Hellman kulcs-csere.
17. Elliptikus görbék és titkosítás segítségükkel.
18. Blokktitkosítók működési módjai.
19. Folyamtitkosítók, az RC4.
20. Üzenethitelesítés általános módszerei, hash és MAC algoritmusok. Születésnap elvű támadások.
21. Hash függvények (MD5, SHA, Whirlpool), HMAC és CMAC üzenethitelesítő küdok. Ezen módszerek biztonsága.
22. Digitális aláírások, visszajátszásos támadások.
23. A Needham-Schroeder protokoll (szimmetrikus kroptográfiával), biztonsága.
24. Kölcsönös hitelesítés szimmetrikus és nyilvános kulcsú kriptográfiával.
25. A DSS szabvány és a DSA algoritmus.
26. Hitelesítés szolgáltatók, X.509 tanúsítványok.
27. Biztonságos e-mailezés, OpenPGP
28. Biztonságos e-mailezés, S/MIME.