Ispitna pitanja na predmetu Sigurnost računalnih sustava
Kriptografske tehničke sigurnosne mjere

1. Navesti vrste napada prema onome što je napadaču dostupno.
2. Navesti definiciju uspješnog napada.
3. Navesti vrste implementacijskih napada.
4. Koje svojstvo DES kriptosustava ga čini nesigurnim?
5. Koji je cilj diferencijalne/linearne kriptoanalize?
6. Diferencijalna kriptoanaliza temelji se na kojim razilkama?
7. Ako je ulaz u neku substitucijsku tablicu 16 bitni podatak, a izlaz su brojevi od 0 do 1023, koliki je broj mogućih razlika na ulazu, a koliki na izlazu?
8. Zašto je napad diferencijalnom kriptoanalizom na kriptosustav DES neuspješan?
9. Ako je linearna transormacija P [1, 4, 13] ⊕ C [1, 2, 3, 4, 6, 9, 11] = K [5, 6, 8] za neki kriptosustav 100% točna (vrijedi uvijek), za koliko bitova se smanjuje prostor ključa?
10. Opisati problem diskretnog logaritma za eliptičke krivulje.
11. Opisati postupak razmjene ključa prokolom ECDH.
12. Obrazložiti zašto je ECDH postupak razmjene tajnog ključa neotporan na napad „Čovjek u sredini".
13. Opisati postupak generiranja ključeva u kriptosustavu EC ElGamal.
14. Usporediti veličine ključeva u kriptosustavima RSA i ECC.
15. Neki moderni kriptosustav koristi ključ veličine N bita i pruža „n-bitnu sigurnost". Pojasniti zašto brojevi N i n ne moraju biti jednaki.
16. Koliko je puta otprilike sporije kriptiranje/dekriptiranje algoritmom RSA1024 od kriptiranja/dekriptiranja algoritmom AES128?
17. Koje sve veličine sažetka mogu generirati kriptografski algoritmi SHA-2 i SHA-3?
18. Spužvasta konstrukcija algoritma SHA-3 sastoji se od sljedeće dvije faze:
19. Što predstavljaju kratice DSS i DSA u postupku digitalnog potpisivanja.
20. Koji se asimetrični kriptoalgoritam koristi u postupku digitalnog potpisivanja DSA?
21. Zašto su kolizije opasne i onda kada izvorne datoteke izgledaju kao slučajni nizovi?
22. Navesti preporučene veličine ključeva i sažetaka: simetrični ključ _____, veličina asimetričnih ključeva (privatni i javni): _____, veličina sažetka: _____.
23. Navesti četiri važna svojstva koja bi trebala zadovoljavati idealna funkcija za izračunavanje sažetka poruke.
24. Opisati svojstvo otpornosti na kolizije.
25. Opisati svojstvo difuzije koje bi svaka funkcija za izračunavanje sažetka poruke (*hash* funkcija) morala zadovoljavati.
26. Opisati napad tablicama s unaprijed izračunatim sažecima (*eng. Rainbow table*).
27. Koje sigurnosne zahtjeve osiguravaju postupci autentifikacijskog kriptiranja?
28. Opisati postupke autentifikacijskog kriptiranja koji koriste MAC (*Message Authentication Code*): EtM, E&M, MtE.
29. Što je elektronički potpis?
30. Kako mogu kvantna računala narušiti sigurnost asimetričnih kriptosustava?
31. Čemu služi QKD protokol?
32. Navesti naziv prvog QKD protokola?
33. Koja dva kanala za razmjenu informacija koristi QKD protokol?
34. Opisati protokol BB84 razmjene ključa.
35. Na koliko načina se mogu polarizirati fotoni u protokolu BB84?
36. Navesti nedostatke protokola BB84.