Nabor izpitnih vprašanj pri predmetu Varne komunikacije

januar 2012

1. Kako imenujemo vidik celovitosti pri prenosu sporočil, ki zagotavlja pritrdilen odgovor na vprašanje:
    a. Ali je vsebina sporočila res dostopna samo naslovniku ?
    b. Ali je sprejeto sporočilo res enako oddanemu sporočilu ?
    c. Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
    d. Ali lahko pošiljatelj zanika avtorstvo sporočila ?
2. Naštejte lastnosti dobrega šifrirnega postopka, ki nam bo omogočil varovanje tajnosti sporočila.
3. Kakšna je razlika med simetričnim in asimetričnim šifrirnim postopkom ?
4. Kaj je slabost asimetričnega šifrirnega postopka v primerjavi s simetričnim ?
5. Kaj je mešani postopek šifriranja in zakaj ga uporabljamo?
6. Kaj so enosmerne funkcije in zakaj jih uporabljamo pri šifriranju sporočil ?
7. Kako imenujemo drugače tudi digitalni prstni odtis sporočila ?
8. Kakšne lastnosti mora imeti zgoščevalna funkcija ?
9. Kaj je digitalni podpis?
10. Katere vidike celovitosti pri prenosu sporočila nam zagotavlja digitalni podpis ?
11. V čem je razlika v uporabi zasebnih in javnih ključev in kje lahko nastopijo problemi ?
12. Kako zagotovimo verodostojnost javnih ključev ?
13. Kakšna je razlika med javnim ključem in digitalnim potrdilom ?
14. Kako delimo klasične šifrirne postopke ?
15. V čem je razlika med transpozicijskim in substitucijskim šifriranjem ?
16. Kakšen postopek šifriranja je uporabljal Julij Cezar ?
17. Kako delimo šifrirne postopke glede na dolžino sporočil, ki jih hkrati šifriramo ?
18. Kaj je prednost pretočnih šifrirnih postopkov v primerjavi z bločnimi ?
19. Ali na šifropis vpliva tudi rezultat šifriranja predhodnih blokov (ECB, CBC, CFB, OFB) ?
21. Koliko bitov je najbolj pogosto v enem bloku ?
22. Kakšne so osnovne značilnosti DES algoritma?
23. Kaj je 3DES ?
24. Kakšne verzije 3DES algoritma poznate ?
25. Kaj je značilnost Feistelove šifre ?
26. Kako poteka generacija ključev za več krogov DES algoritma ?
27. Kakšna je razlika med DES šifrirnim in dešifrirnim algorimom ?
28. Naštejte imena vsaj treh simetričnih šifrirnih postopkov !
29. Kaj je matematična osnova za algoritem RSA ?
30. Razložite postopek generacije RSA ključev !
31. Kako poteka RSA šifriranje ?
32. Kako poteka RSA dešifriranje ?
33. Z javnim ključem (n=527, e=61) šifrirajte čistopis m=40 !
34. Čemu služi postopek Diffie-Hellman?
35. Na čem temelji varnost DH algoritma ?
36. Razložite DH algoritem izmenjave ključev !
37. Kako delimo zgoščevalnih funkcije glede na uporabo tajnega ključa ?
38. Skicirajte model, ki ponazarja princip delovanja iteracijske zgoščevalne funkcije na zaporedju blokov sporočila!
39. V kateri razred spadajo zgoščevalne funkcije MASH1, DES-DaviesMeyer, MD4 in MD5 ? (blokovne, z modularno aritmetiko ali namenske ?)

40. Izvleček pri algoritmu (MD4 , MD5, SHA-1, SHA-2) je dolg: (64, 128, 160, 224, 256, 384, 512 ali 1024) bitov ?
41. Kaj nam zagotavlja digitalni podpis ?
42. Do kakšnih problemov lahko pride pri neurejeni distribuciji javnih ključev ?
43. Kaj je slabost sistema modela neposrednega zaupanja (izmenjav javnih ključev parov uporabnikov)?
44. V čem je razlika med CA in RA ?
45. Katere informacije vsebuje digitalno potrdilo ?
46. Kakšen je standardni format digitalnega potrdila ?
47. Razvrstite protokole za varno komunikacijo po internetu po plasteh od najnižje k najvišji: https, IPSec, SSL
48. V čem je razlika med transportnim in tunelskim načinom delovanja IPSec ?
49. Kaj je SSL ?
50. Ali je kakšna povezava med SSL in TSL ?
51. SSL omogoča preverjanje identitete :na strani klienta ali na strani strežnika
52. Kaj je MIME in kaj je S/MIME ?
53. Kaj je glavna razlika x.509 in PGP certifikatov?
54. Naštejte varnostne mehanizme v radijskem omrežju GSM !
55. Opišite postopek avtentikacije mobilnega terminala v omrežje GSM!
56. Za katere namene se uporabljajo šifrirni algoritmi A3, A5 in A8 ?
57. Naštejte varnostne mehanizme v sistemu TETRA !
58. Kaj pomeni vzajemna avtentikacija mobilnega terminal in bazne postaje?

Vprašanja iz vaj:

59. Pri 'dobremu' algoritmu za šifriranje, koliko bitov šifropisa se spremeni pri spremembi enega bita čistopisa?
60. Kateri del DES algoritma povzroča difuzijo spremembe enega bita čistopisa?
61. Katera je pomanjkljivost ECB blokovnega šifriranja?
62. Od česa je odvisna stopnja varnosti RSA šifrirnega postopka?
63. Opišite pomanjkljivost uporabe majhnega javnega ključa e pri šifriranju v skladu z RSA algoritmom.
64. Kateri algoritem je računsko zahtevnejši RSA ali DES?
65. Katera je pomanjkljivost šifriranja z javnim ključem v primeru omejenega nabora čistopisov?
66. Kako poteka napad na asimetrično šifrirana sporočila s prestrezanjem komunikacije?
67. Kakšna je distribucija prstnih odtisov velikega števila sporočil?
68. Opišite tri pristope napadov na gesla. Utemeljite, kateri pristop je najbolj učinkovit pod danimi pogoji.
69. Kakšno je varno geslo?
70. Katere občutljive informacije s stališča varnosti so lahko shranjene v spletnih piškotkih?
71. Kaj je to »napad človeka v sredini« in na kakšen način se pred tem napadom najlažje zavarujemo pri uporabi spletnih storitev?
72. Zakaj je potrebno javni ključ objaviti na javnem mestu?
73. Zakaj je potrebno zasebni ključ skrbno varovati?
74. Oseba A pošlje sporočilo osebi B. Opišite vsa opravila, ki so potrebna, da oseba B prebere izvorno sporočilo prepričana, da je sporočilo poslala prav oseba A.
75. Oseba A pošlje sporočilo osebi B. Opišite vsa opravila, ki so potrebna, da oseba B prebere izvorno sporočilo prepričana, da morebiten prisluškovalec ne pozna vsebine sporočila.