Nabor vprašanj pri predmetu Kompresija in kriptologija : (Varne komunikacije)

maj 2005

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. Kakšne so osnovne značilnosti DES algoritma?
22. Kaj je 3DES ?
23. Kakšne verzije 3DES algoritma poznate ?
24. Kaj je značilnost Feistelove šifre ?
25. Kako poteka generacija ključev za več krogov DES algoritma ?
26. Kakšna je razlika med DES šifrirnim in dešifrirnim algorimom ?
27. Kaj je rezultat, če v naslednjo permutacijsko tabelo pošljemo zaporedje: 101010101010

Bit	***0***	***1***	***2***	***3***
1	2	6	8	3
5	9	7	10	11
9	5	1	12	4

28. Naštejte osnovne značilnosti AES algoritma !
29. Naštejte imena petih simetričnih šifrirnih postopkov !
30. Kaj je matematična osnova za algoritem RSA ?
31. Razložite postopek generacije RSA ključev !

32. Kako poteka RSA šifriranje ?
33. Kako poteka RSA dešifriranje ?
34. Na osnovi tajnih praštevil (p=11, q=7) izberemo ključ **e**=23. Izračunajte pripadajoči RSA ključ **d** !
35. Z javnim ključem (n=527, e=61) šifrirajte čistopis m=50 !
36. Čemu služi postopek Diffie-Hellman?
37. Na čem temelji varnost DH algoritma ?
38. Razložite DH algoritem izmenjave ključev !
39. Podana sta parametra (g=19, p=31) in tajna ključa uporabnikov ***tkA***=3, ***tkB***=6. Po DH algoritmu izračunajte javna ključa uporabnikov (***jkA***, ***jkB***) in skupni tajni ključ ***tkAB***!
40. Razložite osnovne značilnosti ElGamal algoritma!
41. Kako delimo zgoščevalnih funkcije glede na uporabo tajnega ključa ?
42. Skicirajte model, ki ponazarja princip delovanja iteracijske zgoščevalne funkcije na zaporedju blokov sporočila!
43. V kateri razred spadajo zgoščevalne funkcije MASH1, SHA-1, DES-DaviesMeyer, MD4, MD5 ?
    a. blokovne,
    b. z modularno aritmetiko,
    c. namenske
44. Povzetek pri algoritmu (MD4 , MD5, SHA-1) je dolg:
    a. 128 bitov
    b. 160 bitov
    c. 192 bitov
    d. 256 bitov
45. Kaj je DSA in na čem temelji ?
46. Kaj nam zagotavlja digitalni podpis ?
47. Do kakšnih problemov lahko pride pri neurejeni distribuciji javnih ključev ?
48. Kaj je slabost sistema modela neposrednega zaupanja (izmenjav javnih ključev parov uporabnikov)?
49. V čem je razlika med CA in RA ?
50. Katere informacije vsebuje digitalno potrdil ?
51. Kakšen je standardni format digitalnega potrdila ?
52. Razvrstite protokole za varno komunikacijo po internetu po plasteh od najnižje k najvišji: SHTTP, IPSec, TSL
53. V čem je razlika med transportnim in tunelskim načinom delovanja IPSec ?
54. Kaj je SSL ?
55. Kaj je TSL ?
56. Ali je kakšna povezava med SSL in TSL ?
57. SSL omogoča preverjanje identitete :
    a. na strani klienta
    b. na strani strežnika
58. Na kateri plasti deluje protokol SHTTP?
59. SHTTP omogoča preverjanje identitete :
    a. na strani klienta
    b. na strani strežnika
60. Kaj je MIME in kaj je S/MIME ?
61. Kakšna je razlika med standardi PEM in MOSS ?
62. Ali je PGP simetričen postopek, asimetričen ali kombinacija obeh?
63. Kaj je glavna razlika med X.509 in PGP certifikati?
64. Naštejte vsaj en simetrični in en asimetrični šifrirni postopek, ki se uporablja pri PGP protokolu !

65. Kateri protokol se najpogosteje uporablja za avtentikacijo, avtorizacijo in zaračunavanje storitev?
66. Jedro omrežja WLAN, ki skrbi za prijavo, odjavo, avtentikacijo, avtorizacijo in zaračunavanje storitev je sestavljeno iz usmerjevalnika, strežnika RADIUS in podatkovne baze o uporabnikih. Kateri element omrežja odjavi uporabnika, ko se mu izprazni račun?
67. S čim se uporabnik predstavi, če zaščitena internetna stran zahteva SSL avtentikacijo?
68. Katera sta osnovna gradnika WLAN omrežij pri klasični arhitekturi?
69. Katera dva standarda 802.11x sta med seboj popolnoma združljiva in se razlikujeta po hitrosti?
70. Kaj je WEP?

Dodatni nabor vprašanj iz laboratorijskih vaj:

71. Navedite vsaj tri zahteve za izvedljivost zgoščevalne funkcije!
72. Kakšna je razlika med MD5 in SHA-1 ter HMAC MD5 in HMAC SHA-1 zgoščevalnimi funkcijami?
73. Naštejte vsaj tri primere uporabe zgoščevalne funkcije!
74. Zakaj in kje smo potrebovali statistično analizo jezika (frekvenčna analiza) in kaj smo ugotovili?
75. Kaj je Vigenerjeva šifra?
76. Kaj je in zakaj se uporablja Vigenerjev kvadrat?
77. Zakaj se uporablja LFSR? Navedite primer praktične uporabe!
78. Kakšna je razlika med Vigenerjevo šifro in Vigenerjevo šifro z avtoključem? Narišite oba primera z avtoključem!
79. Dolžina naslova v protokolu IPv6 (verzija 6) je
    a. 32 bitov
    b. 64 bitov
    c. 128 bitov
    d. 256 bitov
80. Napišite omrežno masko poljubne naprave v IP omrežju!
81. Naslov omrežja 213.9.10.64/26 lahko zapišemo tudi kot:
    a. 213.9.10.64 255.255.255.0
    b. 213.9.10.64 255.255.255.26
    c. 213.9.10.64 255.255.255.128
    d. 213.9.10.64 255.255.255.192
    e. 213.9.10.64 255.255.255.230
82. V IPsec uporabljamo za zagotavljanje varnosti dva t.i. protokola varnosti, ki skrbita za avtentikacijo glave paketa in podatkov ter za šifriranje podatkov. Katera sta ta dva protokola?
83. Naštejte tri možnosti uporabe protokola IPsec!
84. Kaj pomeni kratica AAA?
85. Pri preverjanju uporabnika s pomočjo protokola RADIUS si odjemalec (dostopovna točka, ki preverja uporabnika) in strežnik RADIUS izmenjata sporočila, ki poleg uporabniškega imena in gesla lahko vsebujejo še druge parametre (t.i. atributi RADIUS). Čemu služijo ti parametri?

86. Če v spodnjo permutacijsko tabelo

Bit	**0**	**1**	**2**
1	6	5	4
4	3	2	1

pošljemo zaporedje **110010**, dobimo: **010011**
Kakšna je permutacijska tabela, če iz zaporedja **101101** dobimo zaporedje **111100**?

Bit	**0**	**1**	**2**
1	?	?	?
4	?	?	?

87. Kolikokrat se ponovi jedrna funkcija DES algoritma? Zakaj?
88. Čemu služi t.i. »prstni odtis« javnega ključa, ki je sestavni del digitalnega potrdila?
89. Čemu v protokolu PGP služi simetrični šifrirni postopek in čemu asimetrični?
90. Kako pridobimo PGP digitalno potrdilo?
91. Kaj je priložnostno oziroma »ad hoc« WLAN omrežje?
92. Na katerem frekvenčnem področju deluje standard 802.11b in na katerem 802.11g?
93. Zakaj je WPA varnostni mehanizem veliko boljši od WEP mehanizma?