Nabor izpitnih vprašanj pri predmetu Varne komunikacije

januar 2013

1. Kako imenujemo vidik celovitosti pri prenosu sporočil, ki zagotavlja pritrdilen odgovor na vprašanje:

a. Ali je vsebina sporočila res dostopna samo naslovniku?
   - Zasebno ali tajno (privacy, confidentiality)

b. Ali je sprejeto sporočilo res enako oddanemu sporočilu?
   - Verodostojnost

c. Ali nam sporočilo res pošilja predstavljeni pošiljatelj?
   - Avtentičnost

d. Ali lahko pošiljatelj zanika avtorstvo sporočila?
   - Neovrgljivost

2. Naštejte lastnosti dobrega šifrirnega postopka, ki nam bo omogočil varovanje tajnosti sporočila.
   - zasebnost ne sloni na tajnosti postopka ampak na tajnosti ključa za dešifriranje
   - postopek šifriranja mora biti izvedljiv na računalniku v realnem času
   - postopek dešifriranja mora biti izvedljiv na računalniku v realnem času za tistega, ki pozna dešifrirni ključ
   - postopek dešifriranja ne sme biti izvedljiv v realnem času za napadalca, ki ne pozna ključa, čeprav ima zmogljiv računalnik

3. Kakšna je razlika med simetričnim in asimetričnim šifrirnim postopkom?
   - simetrično: uporabimo isti ključ za šifiranje in dešifriranje
   - asimetrično: uporabimo različna ključa, za šifriranje uporabimo javni ključ prejemnika, za dešifriranje pa zasebni tajni ključ

4. Kaj je slabost asimetričnega šifrirnega postopka v primerjavi s simetričnim?
   - preslikava v nasprotni smeri je nemogoča

5. Kaj je mešani postopek šifriranja in zakaj ga uporabljamo?
   - uporabimo simetrični ali asimetrični postopek šifriranja
   - asimetrini postopek uporabimo za izmenjavo začasnega sejnega ključa
   - s sejnim ključem šifriramo in dešifriramo sporočilo
   - uporabimo ga za zagotavljanje bolše varnosti

6. Kaj so enosmerne funkcije in zakaj jih uporabljamo pri šifriranju sporočil?
   - so osnovni gradniki večine protokolov
   - enostavne za izračun
   - preslikava v nasprotni smeri je nemogoča

7. Kako imenujemo drugače tudi digitalni prstni odtis sporočila?
   - izvleček

8. Kakšne lastnosti mora imeti zgoščevalna funkcija?
   - preslika poljubno dolgo sporočilo v blok podatkov končne dolžine
   - je enosmerna
   - možnost da najdemo sporočilo z enakim prstnim odtisom mora biti zelo majhna

9. Kaj je digitalni podpis?
   - digitalni podpis je s tajnim ključem šifriran prstni odtis sporočila
   - digitalni podpis je šifriran izvleček besedila

10. Katere vidike celovitosti pri prenosu sporočila nam zagotavlja digitalni podpis?
   - verodostojnost
   - avtentičnost
   - neovrgljivost

11. V čem je razlika v uporabi zasebnih in javnih ključev in **kje lahko nastopijo problemi**?
   - dostop do tajnega ključa varujemo z geslom
   - javni ključ pa mora biti dostopen vsakomur

12. Kako zagotovimo verodostojnost javnih ključev?
   - verodostojnost javnih ključev potrdi urad za overjanje z digitalnim podpisom odgovorne osebe (CA: certification authority)

13. Kakšna je razlika med javnim ključem in digitalnim potrdilom?
   - digitalno potrdilo je overjena kopija javnega ključa

14. Kako delimo klasične šifrirne postopke?
   - substitucijske in transpozicijske

15. V čem je razlika med transpozicijskim in substitucijskim šifriranjem?
   - substitucijski: znake ali skupino znakov nadomestimo z drugimi
   - transpozicijske: spreminjamo vrstni red znakov ali skupin znakov

16. Kakšen postopek šifriranja je uporabljal Julij Cezar?
   - substitucijsko metodo

17. Kako delimo šifrirne postopke glede na dolžino sporočil, ki jih hkrati šifriramo?
   - delimo jih na pretočne in blokovne šifrirne postopke

18. Kaj je prednost pretočnih šifrirnih postopkov v primerjavi z bločnimi?
   - pretočni šifrirni postopki so veliko hitrejši od blokovnih

19. Ali na šifropis vpliva tudi rezultat šifriranja predhodnih blokov (ECB, CBC, CFB, OFB)?
   - ECB: med bloki ni povezav, vsak blok šifriramo ločeno s 64 bitnim ključem
   - CBC: bloki so verižno povezani tako, da vedno šifriramo mešani (XOR) čistopis bloka in šifropis predhodnega bloka

- CFB: šifropis bloka dobimo z mešanjem (XOR) čistopisa in šifropisa predhodnega bloka
- OFB: šifropis bloka dobimo z mešanjem (XOR) čistopisa in zaporednega stanja. Zaporedja blokov dobimo s šifriranjem predhodnjih blokov

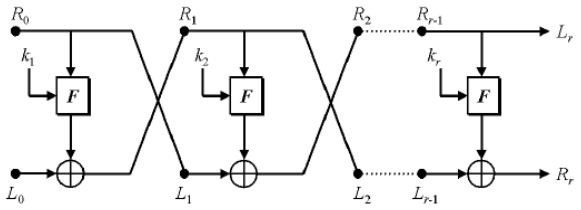
21. Koliko bitov je najbolj pogosto v enem bloku?
    - 64 bitov

22. Kakšne so osnovne značilnosti DES algoritma?
    - ključ ima dolžino 56bitov
    - dolžina bloka je 64 bitov
    - največkrat se uporablja CBC način bločnega šifriranja (CFB & OFB)

23. Kaj je 3DES?
    - trikrat šifriran 64 bitni blok podatkov z različnimi ključi

24. Kakšne verzije 3DES algoritma poznate?
    - E(K1, E(K2), E(K3, P))) , 3 ključi,
    - E(K1, E(K2, E(K1, P)), 2 ključa,
    - E(K1, D(K2, E(K1, P)), 2 ključa,
    - vse tri verzije so enako varne (efektivni 112 bitni ključ)

25. Kaj je značilnost Feistelove šifre?
    - varnost se povečuje s številom krogov prav tako računska kompleksnost
    - nabor ključev izhaja iz istega javnega ključa
    - gre za večkrožno blokovno šifriranje, kjer podatkovni blok razpolovimo na levi in desni del



26. Kako poteka generacija ključev za več krogov DES algoritma?
    - po začetni permutaciji poteka šifriranje v 16 krogih
    - na osnovi 56 bitnega sejanega ključa generiramo 16 podključev K(r)
    - jedro DES algoritma je enkripcijski modul E(1) – E(16)
    - zadnja operacija nad blokom šifriranih podatok je inverzna začetna permutacija

27. Kakšna je razlika med DES šifrirnim in dešifrirnim algorimom?
    - algoritem za dešifriranje je enak algoritmu za šifriranje, le vrstni red pri uporabi podključev se zamenja pri dešifriranju

28. Naštejte imena vsaj treh simetričnih šifrirnih postopkov!
    - DES, AES, NIST, RIJNDAEL, IDEA, Blowfish, Skipjack, CAST…

29. Kaj je matematična osnova za algoritem RSA ?

- RSA izkorišča težavnost faktorizacije velikih števil

30. Razložite postopek generacije RSA ključev!

- izberemo dve veliki praštevili (p,q)
- izračunamo produkt n=p*q (modul)
- izračunamo product phi=(p-1)(q-1)
- izberemo število e, ki nima skupnega faktorja z phi
- poiščemo število d tako, da je pri deljenju producta (e*d) z phi ostanek 1: (e*d)mod(phi)=1
- javni ključ: (n,e)
- tajni ključ: (n,d)

31. Kako poteka RSA šifriranje?

- javni RSA ključ: (n,e)=(527.61)
- sporočilo v čistopisu: m=40
- šifriranje sporočila: $c = E(m) = m^e \bmod n$

$c = 40^{61} \bmod 527$

upoštevamo lastnost: e=61=1+4+8+16+32

$40^1 \bmod 527 = 40$

$40^2 \bmod 527 = (40^1 \bmod 527)^2 \bmod 527 = 19$

$40^4 \bmod 527 = (40^2 \bmod 527)^2 \bmod 527 = 361$

$40^8 \bmod 527 = (40^4 \bmod 527)^2 \bmod 527 = 152$

$40^{16} \bmod 527 = (40^8 \bmod 527)^2 \bmod 527 = 443$

$40^{32} \bmod 527 = (40^{16} \bmod 527)^2 \bmod 527 = 205$

$40^{64} \bmod 527 = (40^{32} \bmod 527)^2 \bmod 527 = 392$

$40^{128} \bmod 527 = (40^{64} \bmod 527)^2 \bmod 527 = 307$

$c = ((40^1 \bmod 527)(40^4 \bmod 527)(40^8 \bmod 527)(40^{16} \bmod 527)(40^{32} \bmod 527)) \bmod 527$

$c = (40*361*152*443*205) \bmod 527 = 350$

-šifrirano sporočilo: c =350

32. Kaj je DSA in na čem temelji?

- DSA (Digital Signature Algorithm) je poseben primer ElGamal algoritma
- varnost temelji na težavnosti računanja diskretnega algoritma

33. Z javnim ključem (n=527, e=61) šifrirajte čistopis m=40!

34. Čemu služi postopek Diffie-Hellman?

- protokol za izmenjavo ključa Diffie-Hellman (1976) je prisoten v večini današnjih protokolov za izmenjavo ključev (IKE, IKEv2, Sigma, JFK, …).
- protokol običajno nastopi v pri fazi z izmenjavo sporočil za generiranje simetričnega ključa

35. Na čem temelji varnost DH algoritma?

- na težavnosti računanja diskretnega algoritma

36. Razložite DH algoritem izmenjave ključev!

-A in B najprej vsak na svoji strani izbereta tajni ključ tk_a in tk_b

-A in B izračunata javna ključa jk_a in jk_b :

$-jk_a = g^{tk(a)} \bmod p$

$-jk_b = g^{tk(b)} \bmod p$

-A in B si izmenjata ključa n_a <--> n_b in izračunata skupni ključ:

-uporabnik A izračuna sejni ključ: $tk_{Ab} = jk_b^{tk(a)} \bmod p$

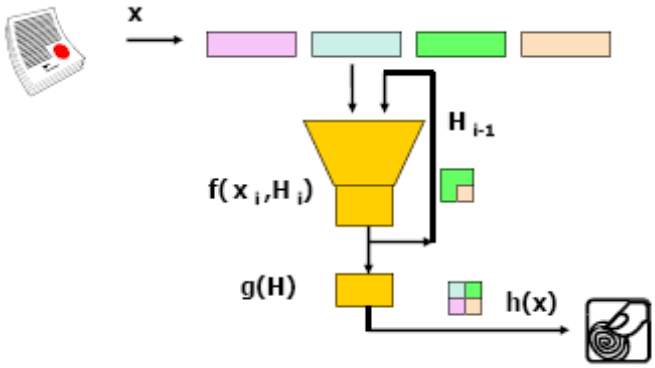
-uporabnik B izračuna sejni ključ: $tk_{Ba} = jk_a^{tk(b)} \bmod p$

-oba sejna ključa sta enaka: $g^{tk(b)\,tk(a)} \bmod p = g^{tk(b)\,tk(a)} \bmod p$

37. Kako delimo zgoščevalnik funkcije glede na uporabo tajnega ključa?

- Delimo jih na MDC (ključa ne potrebujemo) in na MAC (uporablja tajni ključ)

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 ?)

← - blokovne: DES-DaviseMeyer

← - z modulirano aritmetiko: MASH1

← - namenske: MD4, MD5

←

40. Izvleček pri algoritmu (MD4 , MD5, SHA-1, SHA-2) je dolg: (64, 128, 160, 224, 256, 384, 512 ali 1024) bitov?

← - 64 bitov:

← - 128 bitov : MD4, MD5

← - 160 bitov: SHA-1, SHA-2

← - 1024 bitov:

←

41. Kaj nam zagotavlja digitalni podpis?

- Digitalni podpis nam zagotavlja, da je prošiljatelj res tisti od katerega pričakujemo sporočilo

42. Do kakšnih problemov lahko pride pri neurejeni distribuciji javnih ključev?

- javni ključ mora biti vsakemu dostopen, drugače lahko pride do težav:
  - problem lažne identitete: napadalec podtakne lažni javni ključ in dešifrira vsa prestrežena sporočila
  - problem zanikanja identitete: pošiljatelj zanika lastno sporočilo

43. Kaj je slabost sistema modela neposrednega zaupanja (izmenjav javnih ključev parov uporabnikov)?

- javni ključ mora nosti garancijo, da res pripada navedenemu uporabniku

- overjanje javnih ključev opravlja posebna služba, ki skrbi tudi za upravljanje s ključi

44. V čem je razlika med CA in RA?
    - urad za CA potrebuje verodostojnost javnih ključev, z digitalnim podpisom odgovorne osebe
    - uradna oseba RA izvrši identifikacijo

45. Katere informacije vsebuje digitalno potrdilo?
    - kopijo javnega ključa
    - identifikacijske podatke imetnika
    - digitalni podpis urada za overjanje CA
    - datum začetka veljavnosti potrdila
    - datum poteka veljavnosti potrdila
    - serijsko številko

46. Kakšen je standardni format digitalnega potrdila?
    - X.509

47. Razvrstite protokole za varno komunikacijo po internetu po plasteh od najnižje k najvišji: https, IPSec, SSL
    - IPSec
    - SSL
    - HTTPS

48. V čem je razlika med transportnim in tunelskim načinom delovanja IPSec?
    - transportni: ohranja glave paketov nespremenjene, šifrira se samo vsebina paketa
    - tunelski: dodaja novo glavo IP paketom, stara glava in vsebina paketa se prenašata v šifrirani obliki

49. Kaj je SSL?
    - SSL (Secure Socket Layer) je razvil Netscape za varno komunikacijo med spetnim klientom in strežnikom.
    - SSL podpira preverjanje identitete strežnika. V kombinaciji se za vsako sejo ustvari varni kanal.
    - SSL zagotavlja varno komunikacijo na transportni lasti

49. Kaj je TLS?
    - TLS (Transport Layer Security) je standardizirana (IETF)
    zamenjava za SSL.

50. Ali je kakšna povezava med SSL in TSL?
    - TSLv1 in SSLv3 sta si zelo podobna, vendar nista iterperabilna

51. SSL omogoča preverjanje identitete :na strani klienta ali na strani strežnika
    - na strain klienta

52. Kaj je MIME in kaj je S/MIME?

- MIME (multipurpose Internet Mail Extension) je dodatni protocol za izmenjavo podatkov, ki so v ASCII format. Določa nabor funkcij za pretvorbo v ASCII in obratno.
-S/MIME (Secure/Multipurpose Internet Mail Extentions) je varna izboljšava standarda za format elektronske pošte MIME.
    - S/MIME uporablja X-509 infrastrukturo javnih ključev
    - S/MIME je zelo prilagodljiv in omogoča uporabo različnih simetričnih in asimetričnih šifrirnih postopkov

53. Kaj je glavna razlika x.509 in PGP certifikatov?

- X.509 ima hierarhično strukturo
- PGP nima hierarhične strukture

54. Naštejte varnostne mehanizme v radijskem omrežju GSM!

- tajni ključ shranjen na SIM kartici, ki je varovan z dostopnimi kodami PIN in PUK
- identiteta uporabnika je v kombinaciji prikrita: TMSI – IMSI
- avtentikacija mobilne postaje s strain omrežja
- komunikacija na radijskem delu zveze je šifrirana

55. Opišite postopek avtentikacije mobilnega terminala v omrežje GSM!

- tajni ključ K se nikoli ne prenaša po radijskem kanallu
- uporablja se postopek preverjanja po principu challenge - response (RAND>RES)
- v procesu avtentikacije se generira in izmenja skupni tajni ključ DCK
- DCK se uporablja za šifriranje komunikaciji

56. Za katere namene se uporabljajo šifrirni algoritmi A3, A5 in A8?

- Uporabljajo se za šifriranje komunikacij na radijskem linku.

57. Naštejte varnostne mehanizme v sistemu TETRA!

- zagotavljanje avtentičnosti: vzajenma avtentikacija
    - avtentikacija terminal (uporabnika)
    - avtentikacija omrežja
- zagotavljanje tajnosti: šifriranje kombinacij
    - na radijskem kanalu
    - šifriranje med koncema zveze

58. Kaj pomeni vzajemna avtentikacija mobilnega terminal in bazne postaje?

- mobitel preveri omrežje, če je pravo
- omrežje pa preveri, če je mobitel pravi

Vprašanja iz vaj:

59. Pri 'dobremu' algoritmu za šifriranje, koliko bitov šifropisa se spremeni pri spremembi enega bita čistopisa?

- vsi se spreminjajo

60. Kateri del DES algoritma povzroča difuzijo spremembe enega bita čistopisa?
- substitucijski del algoritma

61. Katera je pomanjkljivost ECB blokovnega šifriranja?
- pri ponavljajočih blokih čistopisa dobimo tudi ponavljajoči vzorec v šifropisu

62. Od česa je odvisna stopnja varnosti RSA šifrirnega postopka?
- od velikosti para ključev
- daljši kot so ključi, večja je varnost

63. Opišite pomanjkljivost uporabe majhnega javnega ključa e pri šifriranju v skladu z RSA algoritmom.
- lahko ga kdo prestreže in hitro dekodira

64. Kateri algoritem je računsko zahtevnejši RSA ali DES?
- RSA
- DES je veliko preprostejši in hitrejši od RSA

65. Katera je pomanjkljivost šifriranja z javnim ključem v primeru omejenega nabora čistopisov?
-V primeru majhnega števila možnih čistopisov lahko napadalec na osnovi »znanega čistopisa« in objavljenega šifropisa poskuša z ugibanjem tajnega ključa. Če uspe je seveda tajnost komunikacije trajno izgubljena.

66. Kako poteka napad na asimetrično šifrirana sporočila s prestrezanjem komunikacije?
- na osnovi »znanega čistopisa« in objavljenega šifropisa poskuša z ugibanjem tajnega ključa

67. Kakšna je distribucija prstnih odtisov velikega števila sporočil?
- Distribucija je linearna oziroma enakomerna

68. Opišite tri pristope napadov na gesla. Utemeljite, kateri pristop je najbolj učinkovit pod danimi pogoji.
-napad s surovo silo
-napad na podlagi slovarja
-napad na podlagi mavričnih tabel

69. Kakšno je varno geslo?
- Varno gleso je sestavljeno iz številk, malih in velikih črk(po moznosti se boljše če uporabljaš anglesko abecedo)

70. Katere občutljive informacije s stališča varnosti so lahko shranjene v spletnih piškotkih?
- uporabnikovo avtentikacijo
- stanje uporabniške seje
- uporabniške nastavitve

- s krajo piškotkov lahko napadalec ogrozi zasebnost spletnega uporabnika

71. Kaj je to »napad človeka v sredini« in na kakšen način se pred tem napadom najlažje zavarujemo pri uporabi spletnih storitev?

- primer: Eva s prisluškovanjem internetnega prometa na nekem omrežju zajame piškotek, preko katerega dobi avtentikacijske podatke uporabnika. Med tem, ko uporabnik uporablja neko storitev se Eva z uporabo piškotka poveže na račun ga ukrade, uporabi v svoj prid oz zlorabi.
- zavarujemo se tako, da uporabljamo protocol HTTPS

72. Zakaj je potrebno javni ključ objaviti na javnem mestu?

- Javni ključ mora biti dostopen (javen) vsakomur z jamstvom, da pripada navedenem uporabniku. Sicer lahko pride do problemov kot so:

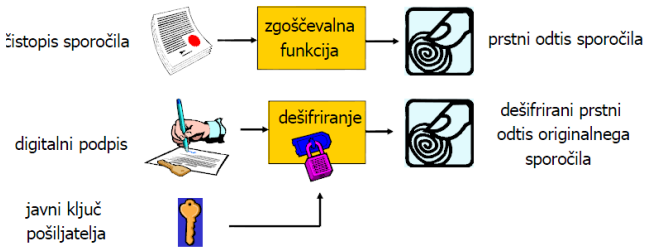
-problem lažne identitete: napadalec podtakne lažni javni ključ i dešifrira vsa prestrežena sporočila

-problem zanikanja identitete: pošiljatelj zanika lastno sporočilo

73. Zakaj je potrebno zasebni ključ skrbno varovati?

- Ker vsak odgovarja za svoj zasebni ključ..zaradi zlorab ne smeš nobenemu zaupati svoj zasebni ključ. namreč če pride do zlorabe, odgovarjaš ti za zlorabo.

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.

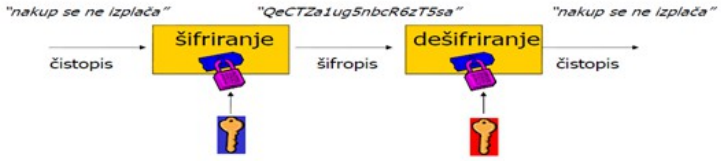


- Prejemnik preveri ujemanje prstnih odtisov in če sta enaka
  - je sporočilo verodostojno,
  - potrjena je identiteta pošiljatelja in
  - pošiljatelj ne more zanikati sporočila.

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.

Asimetrično šifriranje

- Ključa za šifriranje in dešifriranje nista enaka:



- Pošiljatelj šifrira sporočilo z javnim ključem prejemnika.
- Prejemnik dešifrira sporočilo z zasebnim (privatnim) tajnim ključem.
- Asimetrični postopki šifriranja so zasnovani na enosmerni funkciji s stranskim vhodom (one way trapdoor function).