# Varne komunikacije

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

a. Ali je vsebina sporočila res dostopna samo naslovniku ?
Zasebnost ali tajnost (privacy, confidentality)

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

c. Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
Avtentičnost (authentication)

d. Ali lahko pošiljatelj zanika avtorstvo sporočila ?
Neovrgljivost (nonrepudiation)

2. Naštejte lastnosti dobrega šifrirnega postopka, ki nam bo omogočil varovanje tajnosti sporočila.

- Zasebnost ne sloni na tajnosti postopka pač pa na tajnosti ključa za dešifriranje.
- Postopek šifriranja mora biti izvedljiv na računalniku v realnem času.
- Postopek dešifriranja mora 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 razpolaga z zelo zmogljivim računalnikom.

3. Kakšna je razlika med simetričnim in asimetričnim šifrirnim postopkom ?
Pri simetričnem šifriranju uporabimo isti ključ za šifriranje in dešifriranje, pri asimetričnem pa uporabimo različna ključa – za šifriranje se uporabi 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 praktično nemogoča

5. Kaj je mešani postopek šifriranja in zakaj ga uporabljamo?
To je postopek, pri katerem uporabimo simetrični in asimetrični postopek šifriranja – Asimetrični postopek uporabimo za izmenjavo začasnega sejnega ključa, nato pa po simetričnem postopku s sejnim ključem šifriramo in dešifriramo sporočilo. Uporabljamo ga za zagotavljanje večje varnosti??

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

7. Kako imenujemo drugače tudi digitalni prstni odtis sporočila ?
Izvleček (digest)

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

9. Kaj je digitalni podpis?
Digitalni podpis je s tajnim ključem šifrirani prstni odtis sporočila.
Digitalni podpis je šifrirani izvleček besedila

10. Katere vidike celovitosti pri prenosu sporočila nam zagotavlja digitalni podpis ?
Verodostojnost, avtentičnost in neovrgljivost

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

## 12. Kako zagotovimo verodostojnost javnih ključev ?

Verodostojnost javnih ključev potrdi Urad za overjanje (CA=certification authority) z digitalnim podpisom odgovorne osebe

## 13. Kakšna je razlika med javnim ključem in digitalnim potrdilom ?

Digitalno potrdilo je overjena kopija javnega ključa

## 14. Kako delimo klasične šifrirne postopke ?

Delimo jih na substitucijske in transpozicijske

## 15. V čem je razlika med transpozicijskim in substitucijskim šifriranjem ?

Pri substitucijskem znake ali skupino znakov nadomestimo z drugimi
Pri transpozicijskem spreminjamo vrstni red znakov ali skupin znakov

## 16. Kakšen postopek šifriranja je uporabljal Julij Cezar ?

Cezar je uporabljal substitucijsko metodo šifriranja

## 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 predhodnih blokov

## 21. Koliko bitov je najbolj pogosto v enem bloku ?

64 bitov.

## 22. Kakšne so osnovne značilnosti DES algoritma?

Ključ ima dolžino 56 bitov, dolžina bloka je 64 bitov, največkrat se uporablja CBC način bločnega šifriranja (možni tudi CFB in OFB)

## 23. Kaj je 3DES ?

Trikrat šifrira 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 3 verzije so enako varne (efektivni 112 bitni ključ)

## 25. Kaj je značilnost Feistelove šifre ?

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 sejnega ključa generiramo 16 podključev K(r)
- jedro DES algoritma je enkripcijski modul E(1) - E(16)

- zadnja operacija nad blokom šifriranih podatkov je inverzna začetna permutacija

## 27. Kakšna je razlika med DES šifrirnim in dešifrirnim algoritmom ?

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 težavnosti faktorizacije velikih števil

## 30. Razložite postopek generacije RSA ključev !

- izberemo dve veliki praštevili (p,q)
- izračunamo produkt n= p q (modul) ,
- izračunamo produkt $\varphi = (p-1)(q-1)$
- izberemo število e, ki nima skupnega faktorja z $\varphi$
- poiščemo število d tako, da daje produkt (e d) ostanek 1 pri deljenju z $\varphi$: $(e\ d) \bmod \varphi = 1$
- **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 mod 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. Kako poteka RSA dešifriranje ?

- tajni RSA ključ: (n, d)=(527,181)
- sporočilo v šifropisu: c = 350
- dešifriranje sporočila: m = D(c) = c d mod n

$m = 350^{181} \bmod 527$

upoštevamo lastnost: d=181=1+4+16+32+128

$350^1 \bmod 527 = 350$

$350^2 \bmod 527 = (350^1 \bmod 527)^2 \bmod 527 = 236$

$350^4 \bmod 527 = (350^2 \bmod 527)^2 \bmod 527 = 361$

$350^8 \bmod 527 = (350^4 \bmod 527)^2 \bmod 527 = 152$

$350^{16} \bmod 527 = (350^8 \bmod 527)^2 \bmod 527 = 443$

$350^{32} \bmod 527 = (350^{16} \bmod 527)^2 \bmod 527 = 205$

$350^{64} \bmod 527 = (350^{32} \bmod 527)^2 \bmod 527 = 392$

$350^{128} \bmod 527 = (350^{64} \bmod 527)^2 \bmod 527 = 307$

$c = ((350^1 \bmod 527)(350^4 \bmod 527)(350^{16} \bmod 527)(350^{32} \bmod 527)(350^{128} \bmod 527)) \bmod 527$

$c = (350 * 361 * 443 * 205 * 307) \bmod 527 = 40$

- dešifrirano sporočilo: m =40

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

VPRAŠANJE 31

## 34. Čemu služi postopek DiffieHellman?

Protokol, imenovan Diffie-Hellman protokol za izmenjavo in kreiranje ključev, je

kriptografski protokol, ki omogoča dvema ali več strankam, za katere ni nujno da se predhodno poznajo, sestavo skupnega skrivnega ključa preko nezavarovanega komunikacijskega kanala. Ta ključ lahko potem uporabimo za šifriranje sporočil z algoritmom simetričnega šifriranja.

### 35. Na čem temelji varnost DH algoritma ?

Varnost temelji na težavnosti računanja diskretnega logaritma.

### 36. Razložite DH algoritem izmenjave ključev !

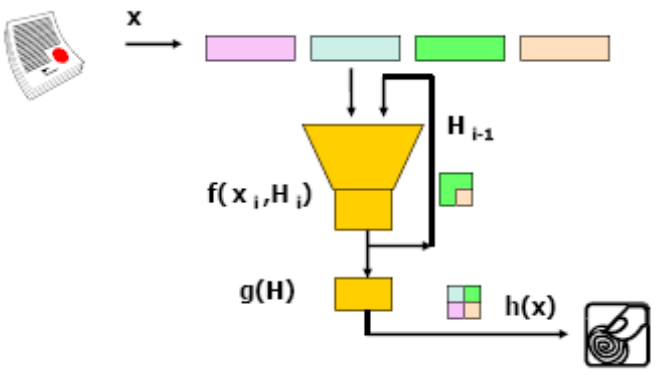
A in B najprej vsak na svoji strani izbereta tajni ključ tka in tkb

- A in B izračunata javna ključa jka in jkb :
- jka =gtk(a) mod p
- jkb =gtk(b) mod p
- A in B si izmenjata ključa na <--> nb in izračunata skupni ključ:
- uporabnik A izračuna sejni ključ: tkAb = jkb
  tk(a) mod p
- uporabnik B izračuna sejni ključ: tkBa = jka
  tk(b) mod p
- oba sejna ključa sta enaka: gtk(b) tk(a) mod p = gtk(b) tk(a) mod p

### 37. Kako delimo zgoščevalnih 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, DESDaviesMeyer, MD4 in MD5 ?

a. blokovne: DESDaviesMeyer
b. z modularno aritmetiko: MASH1
c. namenske: MD4, MD5

### 40. izvleček pri algoritmu (MD4 , MD5, SHA1) je dolg:

a. 64 bitov
b. 128 bitov: MD4, MD5
c. 160 bitov: SHA1
d. 1024 bitov:

### 41. Kaj nam zagotavlja digitalni podpis ?

Digitalni podpis nam zagotavlja, da je pošiljatelj res tisti od katerega pričakujemo sporočilo.

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

Javni ključ mora biti vsakomur 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 )?
Uporabniki si v parih izmenjajo certifikate.

### 44. V čem je razlika med CA in RA ?
Urad za overjanje (CA) potrjuje 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, TSL
IPSec, TSL, 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 spletnim klientom in strežnikom. SSL podpira preverjanje identitete strežnika. V komunikaciji se za vsako sejo ustvari varni kanal. SSL zagotavlja varno komunikacijo na transportni plasti.

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

### 50. Ali je kakšna povezava med SSL in TSL
TLS_v1 in SSL_v3 sta si zelo podobna, vendar nista interoperabilna

### 51. SSL omogoča preverjanje identitete :
a. na strani klienta
b. na strani strežnika

### 52. Kaj je MIME in kaj je S/MIME ?
MIME (Multipurpose Internet Mail Extension) je dodatni protokol za izmenjavo podatkov, ki niso v ASCII formatu. MIME določa nabor funkcij za pretvorbo v ASCII in obratno.

S/MIME je varna izboljšava standarda za format elektronske pošte MIME; uporablja x.509 infrastrukturo javnih ključev, je zelo prilagodljiv in omogoča uporabo različnih simetričnih in asimetričnih šifrirnih postopkov.

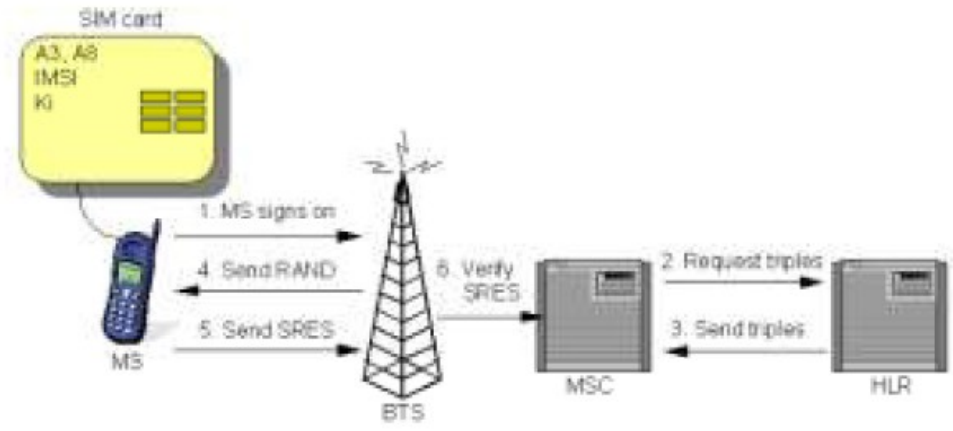
## 53. Kaj je glavna razlika x.509 in PGP certifikatov?

X.509 nima hierarhične strukture, PGP pa jo ima

## 54. Naštejte varnostne mehanizme v radijskem omrežju GSM !

- tajni ključ Ki je shranjen na SIM kartici in varovan z dostopovnimi kodami (PIN, PUK) in se ne prenaša po radijskem kanalu
- identiteta uporabnika je v komunikaciji prikrita: TMSI - IMSI
- avtentikacija mobilne postaje s strani omrežja
- komunikacija na radijskem delu zveze je šifrirana

## 55. Opišite postopek avtentikacije mobilnega terminala v omrežje GSM!



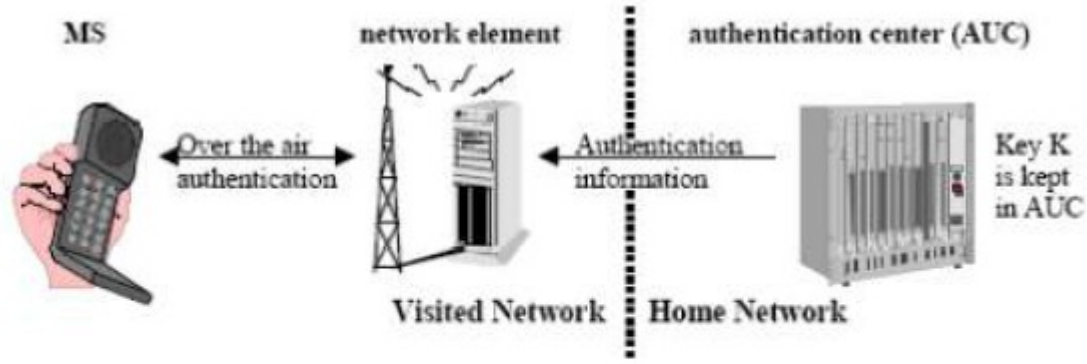

## 56. Za katere namene se uporabljajo šifrirni algoritmi A3, A5 in A8 ?

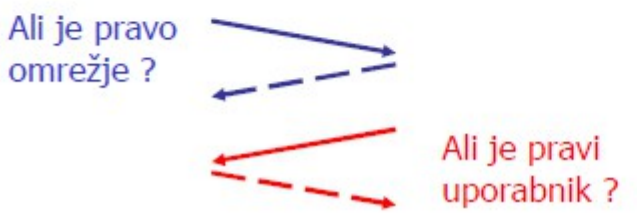
A3 in A8 za avtentikacijo, A5 pa za šifriranje komunikacij na radijskem linku.

## 57. Naštejte varnostne mehanizme v sistemu TETRA !

- zagotavljanje avtentičnosti: vzajemna avtentikacija
  - avtentikacija terminala
  - avtentikacija omrežja
- zagotavljanje tajnosti: šifriranje komunikacij
  - na radijskem kanalu
  - šifriranje med koncema zveze

## 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?

Spremenijo se vsi biti.

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

Difuzijo vnašajo operacije P (permutacije) v algoritmu DES.
Namen difuzije je otežiti napad na osnovi poznavanja statistike čistopisov.

### 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 pri šifriranju v skladu z RSA algoritmom.

Pomanjkljivost je, da ga lahko kdo prestreže

### 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?

### 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.

- Napad s surovo silo
- Napad na podlagi slovarja
- Napad na podlagi mavričnih tabel

## 69. Kakšno je varno geslo?

- Ima čim več različnih znakov
- Ima čim več znakov
- Uporabimo čim boljši algoritem

## 70. Katere občutljive informacije s stališča varnosti so lahko shranjene v spletnih piškotkih?

Uporabnikova avtentikacija, stanje uporabniške seje, uporabniške nastavitve itd.

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

»Napad človeka v sredini« pomeni, da se prisluškuje, spremlja in beleži uporabnikov promet. S prestrežbo avtentikacijskih podatkov lahko povzroči veliko škode. Pred tem napadom se najlažje zavarujemo z uporabo protokola HTTPS.

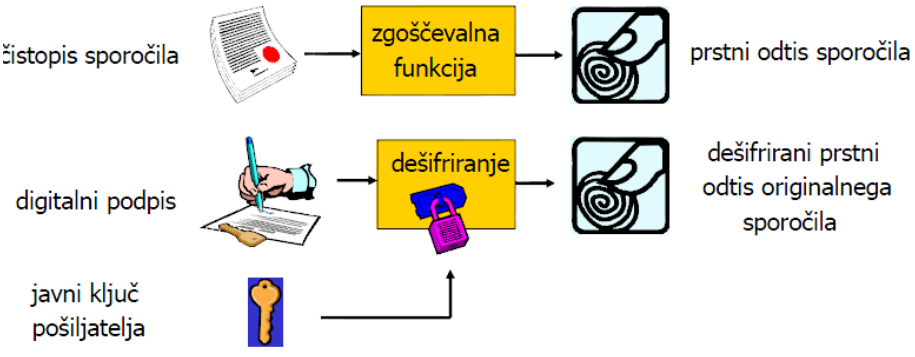
## 72. Zakaj je potrebno javni ključ objaviti na javnem mestu?

Javni ključ mora biti vsakomur dostopen z jamstvom, da pripada navedenemu uporabniku.

## 73. Zakaj je potrebno zasebni ključ skrbno varovati?

»Geslo je kot zobna ščetka, izberi si dobro in je ne posojaj nikomur.« Ker v nasprotnem primeru nosi vso odgovornost za zlorabe.

## 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.

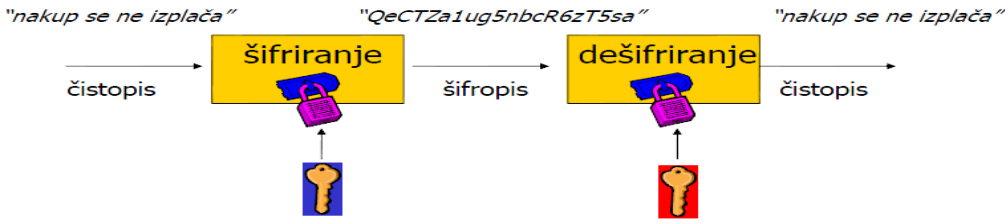



- Prejemnik preveri ujemanje prstnih odtisov in če sta enaka
  - je sporočilo verodostojno,
  - potrjena je identiteta pošiljatelja in
  - pošiljatelj ne more zanikati sporočila.

## 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).