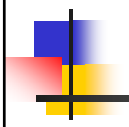


Varnost komunikacij

TKO

Anton Umek

Elektronski in tiskani dokumenti

- Skoraj vsi dokumenti nastajajo s pomočjo računalnika.
- Elektronski dokument ima veliko prednosti:
  - kadarkoli ga lahko ponovno natisnemo
  - lahko ga tudi spreminjamo: spremenimo naslovnika, datum...
- Zakaj se potem velik del dokumentov še vedno tiska na papir ?
- Vprašljiva je originalnost elektronskega dokumenta
- Tiskani dokument vsebuje lastnoročne podpise in časovne žige
- Elektronski dokument brez varnostnih mehanizmov ni pravno veljaven:
  - ne more služiti za arhiv ali kot pogodba

Razvoj izmenjave elektronskih dokumentov

- dokument natisnemo na papir in po pošti pošljemo naslovniku
- dokument pošljemo iz računalnika direktno na telefaks naslovnika
- dokument pošljemo v elektronski obliki na fizičnem mediju (kurir, pošta, DHL..)
- dokument posredujemo v elektronski obliki na primer preko elektronske pošte

- zadnji način je od vseh naštetih najbolj učinkovit vendar hkrati tudi najbolj ranljiv !

Zaupni dokumenti in zasebnost komunikacije

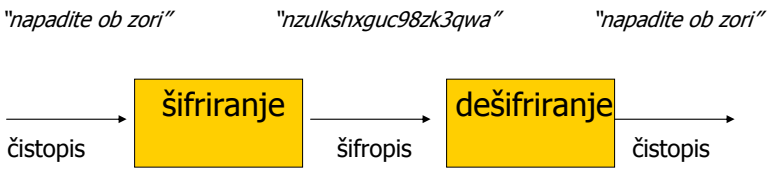
- Zaupni dokument je namenjem samo naslovniku, zato želimo preprečiti vpogled tretje osebe.
- Govorimo o zasebnosti ali tajnosti komunikacije.
- Če zaupni dokument pride v napačne roke je zasebnost komunikacije izgubljena.
- Verjetnost takšnega dogodka je omejena s stopnjo varovanja zasebnosti. Zelo zaupne dokumente varujemo z najvišjo možno stopnjo varovanja zasebnosti (tajnosti).
- Pri pismu je zasebnost udeležencev v komunikaciji slabo varovana z vlaganjem tiskanega dokumenta v ovojnico. Zaupnost tiskanega dokumenta je lahko posebej označena, kar pa lahko še dodatno pritegne pozornost.

Zagotavljanje celovitosti sporočil

- zasebnost ali tajnost:
  - Ali je vsebina sporočila res dostopna samo naslovniku ?
- verodostojnost :
  - Ali je sprejeto sporočilo res enako oddanemu sporočilu ?
- avtentičnost zagotavlja izjavljeno identiteto pošiljatelja:
  - Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
- neovrgljivost:
  - Ali lahko pošiljatelj zanika avtorstvo sporočila ?

Šifriranje dokumentov

- Varovanje zasebnosti zagotovimo s šifriranjem dokumentov tako, da velja:
  - iz šifriranega dokumenta ni mogoče razbrati vsebine in
  - samo naslovnik zna dešifrirati dokument.
- Primer šifriranja teksta:



Zgodovina šifriranja sporočil

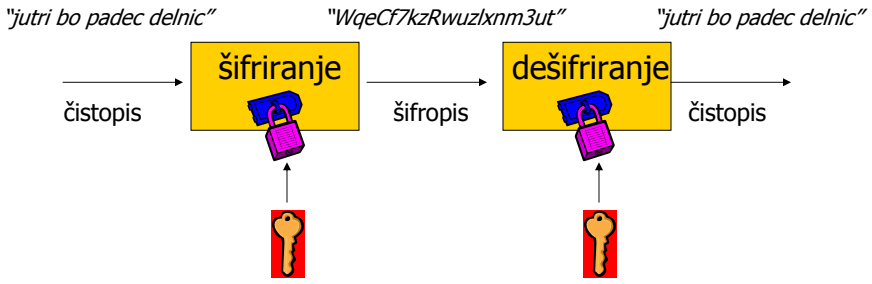
- Veda o šifriranju (kriptologija) je bila zelo dolgo na seznamu najstrožje varovanih skrivnosti
  - Grki: kryptos "skrite" , logos "besede", angl: cryptology
  - Cezarjev postopek šifriranja : CESARUS->FHVDUAV
  - Nemški šifrirni stroj iz II. svetovne vojne: Enigma
- Javno uporabo kriptografije je omogočila iznajdba asimetričnega postopka šifriranja pred približno 30. leti
  - junija 1991 je Philip Zimerman objavil programski paket za varno izmenjavo sporočil PGP (Prety Good Privacy)
  - Danes uporabljamo vrsto standardnih postopkov šifriranja sporočil v privatnih in poslovnih komunikacijah.

Šifrirni postopek

- Lastnosti dobrega šifrirnega postopka:
  - 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.
- Glede na smernost šifrirnega postopka ločimo:
  - Simetrično šifriranje (dvosmerno šifriranje)
  - Asimetrično šifriranje (enosmerno šifriranje)

Simetrično šifriranje

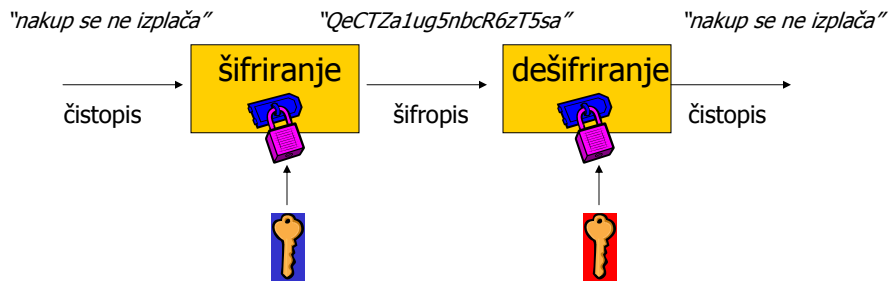
- Za šifriranje in dešifriranje uporabimo enak tajni ključ:



- Primer simetričnih šifrirnih algoritmov: DES, AES

Asimetrično šifriranje

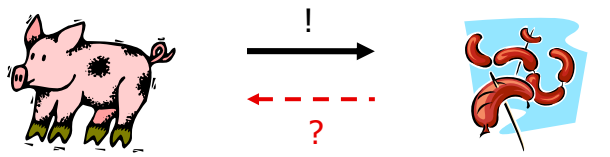
- Ključa za šifriranje in dešifriranje nista enaka:

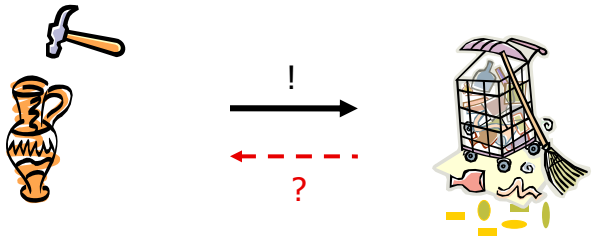


- Pošiljatelj šifrira sporočilo z javnim ključem prejemnika.
- Prejemnik dešifrira sporočilo z zasebnim tajnim ključem.
- Primer asimetričnih šifrirnih algoritmov: RSA, ElGamal...

"Enosmerne funkcije" ☺☺

- Preslikava v nasprotni smeri je praktično nemogoča:





Mešani postopek šifriranja

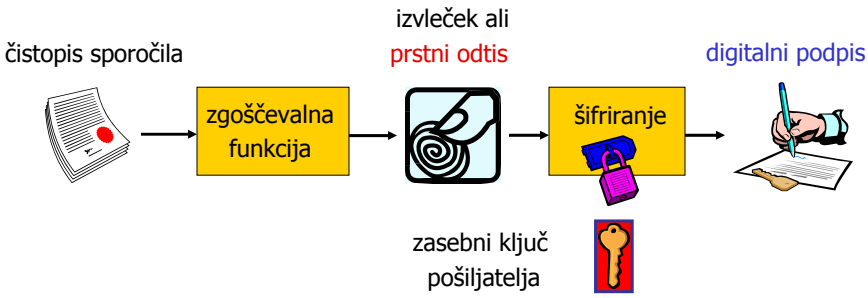
- Asimetrični šifrirni postopek zahteva mnogo več računanja kot simetrični šifrirni postopek. V praktičnih sistemih se zato uporablja mešani postopek šifriranja:
  - Asimetrični postopek uporabimo za izmenjavo začasnega sejnega ključa.
  - Po simetričnem postopku s sejnim ključem šifriramo in dešifriramo sporočilo.
- Pošiljatelj pošlje simetrično šifrirano sporočilo in zraven še asimetrično šifriran ključ, s katerim je bilo sporočilo šifrirano:
  - Pošiljatelj naključno generira sejni ključ in z njim šifrira sporočilo.
  - Ključ s katerim je sporočilo šifrirano se šifrira z javnim ključem naslovnika.
- Prejemnik prejme šifrirano sporočilo in šifriran sejni ključ.
  - Prejemnik dešifrira sejni ključ s svojim privatnim tajnim ključem.
  - Prejemnik na osnovi sejnega ključa dešifrira sporočilo.

Verodostojnost, avtentičnost in neovrgljivost

- Elektronski prstni odtis dokumenta
- Digitalni podpis
- Upravljanje s ključi
- Digitalno potrdilo

Digitalni podpis

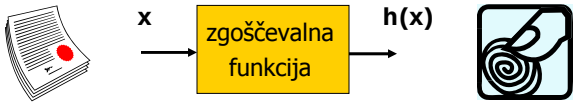
- Digitalni podpis je s tajnim ključem šifrirani prstni odtis sporočila:



- Zgoščevalna funkcija je enosmerna funkcija in vsaka sprememba čistopisa spremeni tudi prstni odtis sporočila.
- Napadalec bi lahko spremenil sporočilo in dodal nov prstni odtis !
- Pošiljatelj zaščiti prstni odtis s šifriranjem!

Zgoščevalna funkcija

- Zgoščevalna funkcija (hash function) preslika poljubno dolgo sporočilo v blok podatkov končne dolžine. Izvleček (digest) imenujemo tudi prstni odtis (digital fingerprint) sporočila.
- Zgoščevalna funkcija je enosmerna funkcija.
- Verjetnost, da najdemo sporočilo z enakim prstnim odtisom mora biti zelo majhna **Pr(** $h(x_1)=h(x_2)$ **) --> 0** .

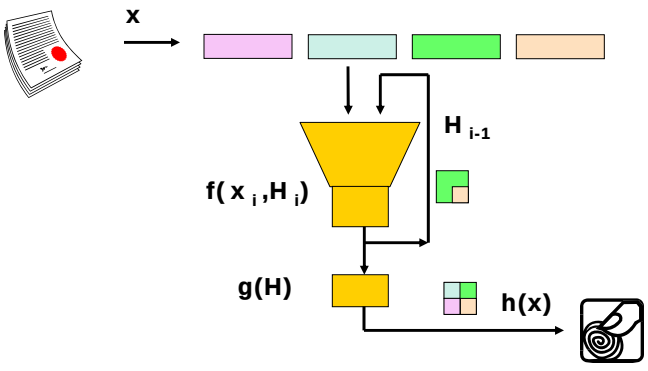


čistopis

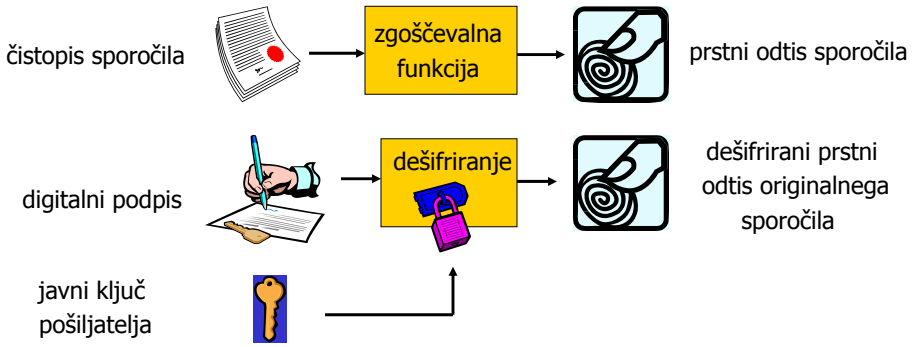
izvleček ali prstni odtis

Model iteracijske zgoščevalne funkcije

- Sporočilo razdelimo na bloke dogovorjene dolžine.
- Postopek zgoščevanja ponavljamo in vsakič uporabimo izvleček predhodnih blokov.



Preverjanje digitalnega podpisa



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

Namen digitalnega podpisa

- Digitalni podpis dodajamo nešifriranemu sporočilu in zato ne zagotavlja tajnosti komunikacije.
- Pošiljatelj z digitalnim podpisom zagotovi:
  - verodostojnost sporočila,
  - potrjuje svojo identiteto in s tem
  - sprejme tudi odgovornost za sporočilo.
- Prejemnik lahko hkrati preveri verodostojnost in avtentičnost:
  - Ali je sprejeto sporočilo res enako oddanemu sporočilu ?
  - Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
- Če prejemnik potrdi verodostojnost sporočila in avtentičnost pošiljatelja, potem tudi pošiljatelj ne more sporočila zanikati:
  - Če se prstna odtisa ujemata, potem sporočilo ni bilo spremenjeno in podpisal ga je lahko le pošiljatelj, ki ima edini pravi zasebni ključ.
- Digitalni podpis omogoča zagotavljanje verodostojnosti, avtentičnosti in neovrgljivosti sporočil.

Uporaba zasebnih in javnih ključev

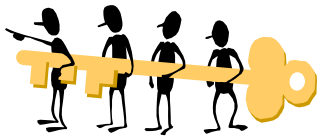
- Digitalni podpis temelji na asimetričnem šifrirnem postopku, ki uporablja parov imetnikovih ključev: javni ključ + zasebni ključ

- Vsak uporabnik nosi odgovornost za uporabo in varovanje zasebnega ključa. Dostop do tajnega ključa varujemo z dolgim geslom, ki ga imenujemo fraza. Uporabnik ne sme zaupati nikomur svojega zasebnega ključa. Če to stori, potem nosi tudi vso odgovornost za zlorabe.

- Javni ključ mora biti vsakomur dostopen z jamstvom, da pripada navedenemu uporabniku. V nasprotnem primeru lahko pride do problemov:
  - Problem lažne identitete: napadalec podtakne lažni javni ključ in dešifrira vsa prestrežena sporočila.
  - Problem zanikanja identitete: pošiljatelj zanika lastno sporočilo.

Upravljanje s ključi

- Javni ključ mora nositi garancijo, da res pripada navedenemu uporabniku. Overjanje javnih ključov opravlja posebna služba (podobno notarju), ki skrbi tudi za upravljanje s ključi.
- Urad za overjanje (**CA**=Certification Authority) potrjuje verodostojnost javnih ključev z digitalnim podpisom odgovorne osebe. Imetnik javnega ključa se mora ob registraciji identificirati in s tem prevzema odgovornost za uporabo zasebnega ključa. Identifikacijo izvrši uradna oseba (RA=Registration Authority).
- Na zahteve imetnikov opravlja CA tudi razveljavitve javnih ključev. Potreba po preklicu javnega ključa nastopi v primeru izgube tajnosti zasebnega ključa.



Digitalno potrdilo

- Digitalno potrdilo (digital certificate) je kopija javnega ključa, ki je overjena od tretje osebe ali institucije.
- Imetnik javnega ključa se mora ob registraciji identificirati in s tem prevzema tudi odgovornost za uporabo zasebnega ključa. Identifikacijo izvrši uradna oseba RA (Registration Authority).
- Urad za overjanje potrdil CA (Certification Authority) je nevtralna organizacija, ki ji uporabniki zaupajo.
- Upravljanje z javnimi ključi ne zajema samo shranjevanje digitalnih potrdil na strežniku, pač pa celoten postopek posrednih overjanj izdajateljev potrdil, razveljavitve javnih ključev itn.
- Infrastruktura javnih ključev PKI (Public Key Infrastructure) določa protokole in storitve pri upravljanju z javnimi ključi.

Format digitalnega potrdila

- Digitalno potrdilo vsebuje poleg javnega ključa tudi množico identifikacijskih podatkov uporabnika in izdajatelja potrdila.
- Najbolj znana formata sta X-509 in PGP:
  - ITU-T mednarodni standard predpisuje X-509 format digitalnih potrdil. V opisu je določeno katere informacije so vsebovane v poljih potrdila in kakšen je njihov format zapisa.
    - X-509 v1 1988, osem polj
    - X-509 v2 1993, + dodani dve identifikacijski polji - 10 polj
    - X-509 v3 1996, + dodano polje za razširitve
  - PGP format digitalnega potrdila se uporablja v programskem paketu za varno izmenjavo podatkov PGP (Pretty Good Privacy). PGP je v začetku devetdesetih let ustvaril Phil Zimmerman.