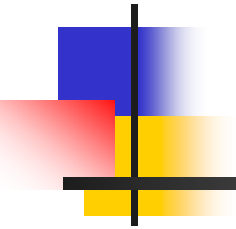
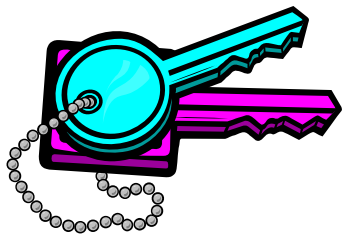


Kompresija in kriptologija
Varne komunikacije

anton.umek@fe.uni-lj.si

Uvod v varne komunikacije

- Elektronski dokumenti
- Izmenjava datotek
- Zasebnost in zaupnost
- Celovitost sporočil
- Šifriranje dokumentov



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 !

Zasebnost in zaupni dokumenti

- Govorimo o zasebnosti ali tajnosti komunikacije.
- Zaupni dokument je namenjem samo naslovniku, zato želimo preprečiti vpogled tretje osebe.
- 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

Poznamo več vidikov celovitosti sporočil:

- zasebnost ali tajnost (privacy , confidentiality)
  - Ali je vsebina sporočila res dostopna samo naslovniku ?
- verodostojnost :
  - Ali je sprejeto sporočilo res enako oddanemu sporočilu ?
- avtentičnost (authentication) zagotavlja izjavljeno identiteto pošiljatelja:
  - Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
- neovrgljivost (nonrepudiation):
  - Ali lahko pošiljatelj zanika avtorstvo sporočila ?
- časovna opredeljenost: časovne omejitve veljavnosti, časovni žig, trajnost !

Šifriranje dokumentov

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

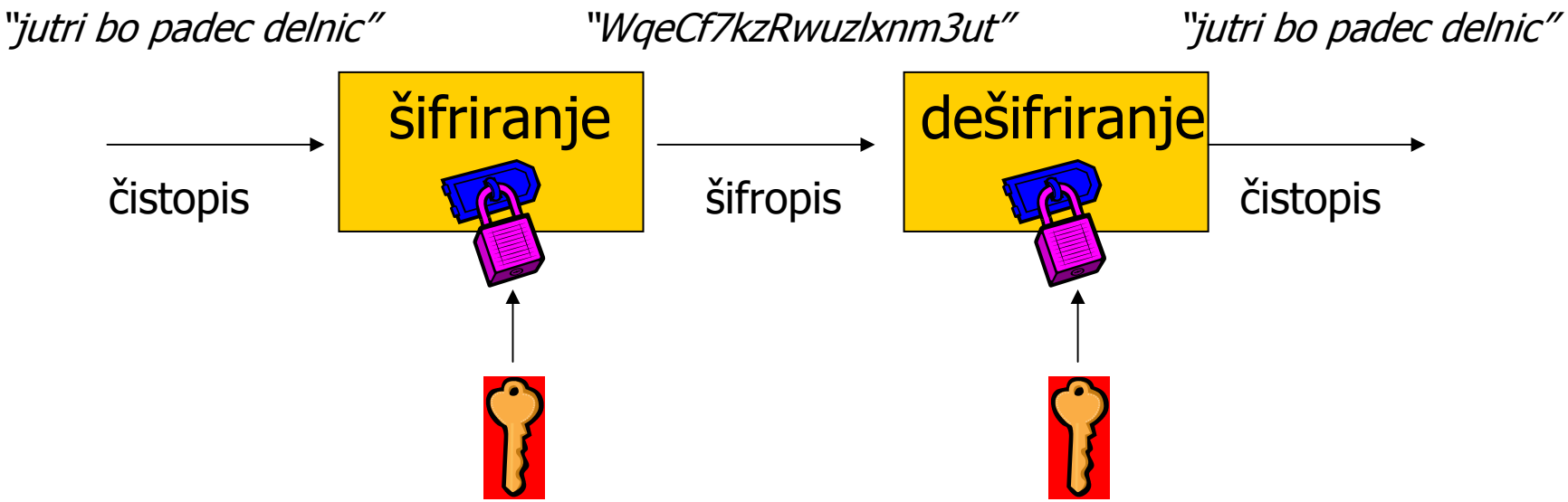
Šifrirni postopek

- 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

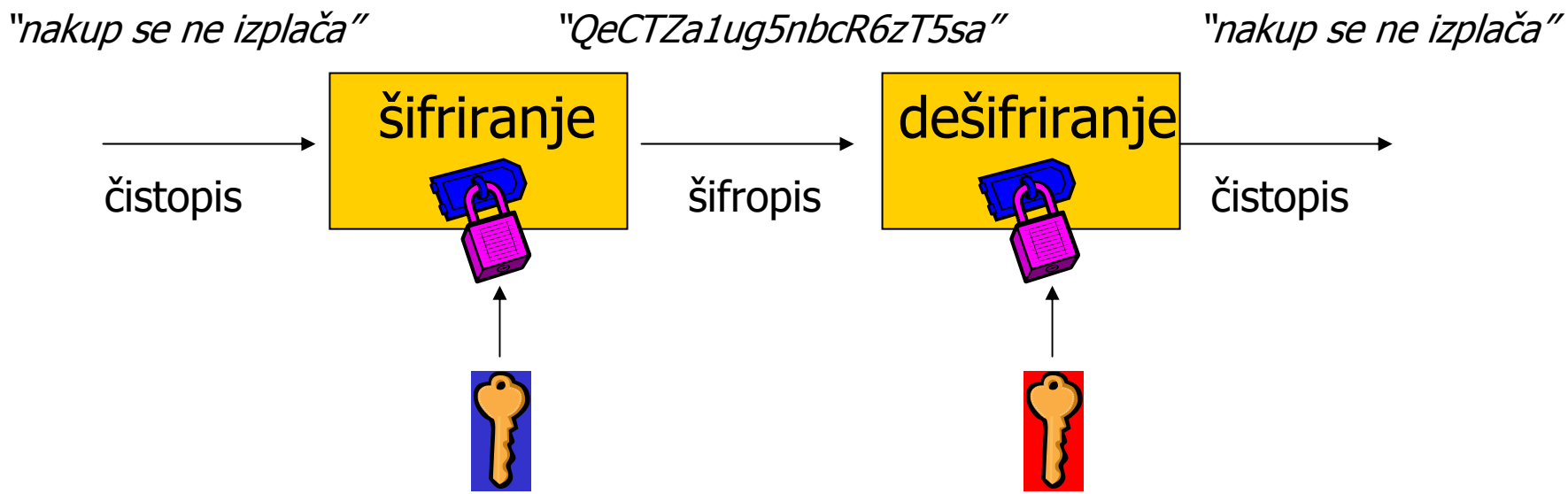
- Za šifriranje in dešifriranje uporabimo isti ključ:



- Pošiljatelj in prejemnik morata uporabiti enak tajni ključ !

Asimetrično šifriranje

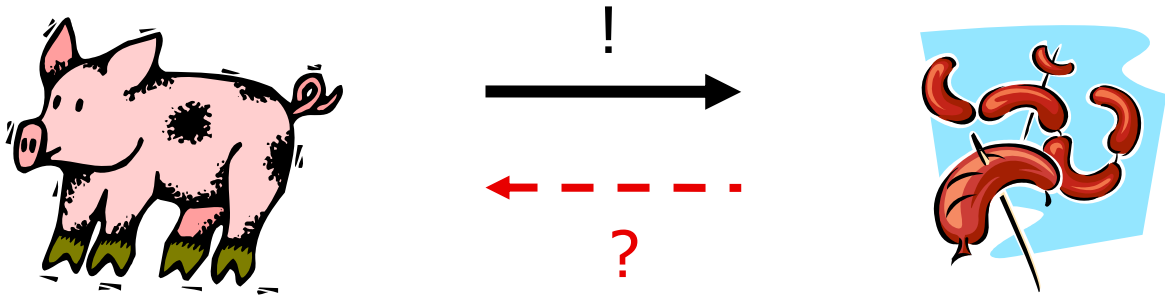
- Ključa za šifriranje in dešifriranje nista enaka:

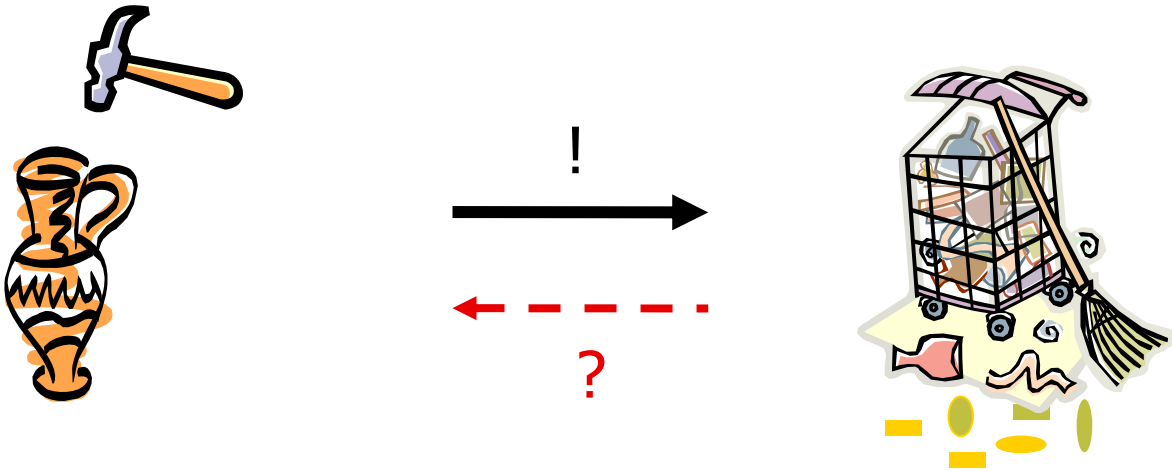


- Pošiljatelj šifrira sporočilo z javnim ključem prejemnika.
- Prejemnik dešifrira sporočilo z zasebnim (privatnim) tajnim ključem.
- Asimetrični postopki šifriranja so zasnovani na enosmerni funkciji s stranskim vhodom (one way trapdoor function).

Enosmerne funkcije

- Preslikava v nasprotni smeri je praktično nemogoča:





Mešani postopek šifriranja

- Uporabimo simetrični in asimetrični 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.