

Kriptografija

Emil Hudomalj, 2002/2003, V1.0

Inštitut za biomedicinsko informatiko

Emil.Hudomalj@mf.uni-lj.si

www2.mf.uni-lj.si/~emil

Kriptografija (skrivnopolisje)

je eden od varnostnih mehanizmov za izpolnitev varnostnih zahtev.

Uporabljen znanja za doseganje ciljev so:

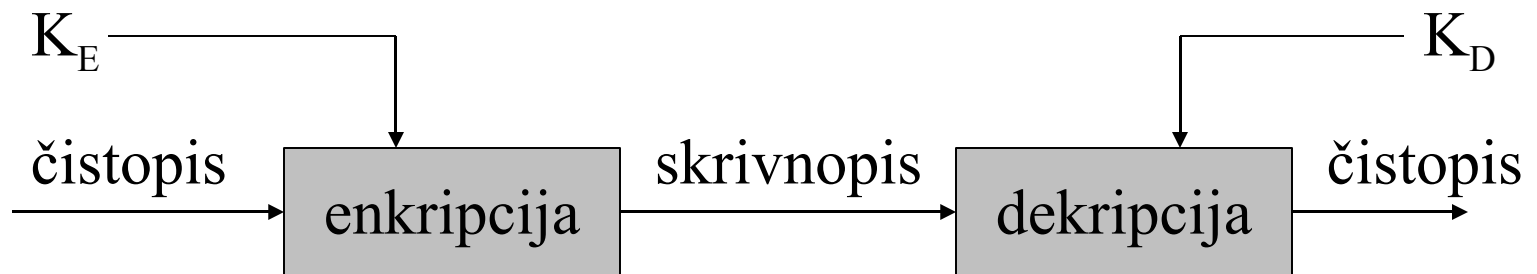
- matematika (zlasti teorija števil)
- računalništvo (analiza algoritmov)
- elektrotehnika (strojna oprema)
- poznavanje aplikacij
- politika, pravo, družba...

Cilji kriptografije

- ugotavljanje verodostojnosti osebe in izvora sporočila
- zagotavljanje zaupnosti podatkov
- zagotavljanje celovitosti podatkov
- zagotavljanje nezatajljivosti

Kriptografski sistemi – delitev glede na lastnosti ključev

- simetrični sistemi (SS): isti ključ se uporabi pri enkripciji in dekripciji ($K_E = K_D$)
- asimetrični sistemi (AS): ključa sta različna



Kriptografski sistemi – delitev na način zakrivanja

- *substitucijski*
- *transpozicijski*
- *enega kot drugega z računalniki enostavno razkrijemo!*

Primer preprostega skrivnopisa

KAČOČ DSJŽ, GČRHU MH ŠHZHN.

Rešitev primera

- Ključ je 3, metoda pa zamik črk v abecedi

A	B	C	Č	D	E	F	G	H	I	...
Č	D	E	F	G	H	I	J	K	L	...

Dešifrirano:

HVALA BOGU, DANES JE PETEK

Primer substitucijskega algoritma

- znake ali skupino znakov nedomestimo z drugimi (npr. Vigenerejev kriptogram, morsejeva koda)
- Cesarjev skrivnopolis (metoda je premik črk, koda je premik za 7)
- Čistopolis:
TO JE MOJE ORIGINALNO SPOROČILO
- Kodirano:
ZU PK SUPK UXOMOTGRTU YVUXUIORU

Primer transpozicijskega algoritma

- *transpozicijski* (permutacijski): spreminjamo vrstni red znakov ali skupin znakov
- Čistopis:
TO JE MOJE ORIGINALNO SPOROČILO
- Kodirano:
OT EJ EJOM ONLANIGIRO OLIČOROPS

Sodobni simetrični kriptografski algoritmi

- delujejo nad nizi bitov, npr. 64
- združujejo vse klasične oblike, ekspanzije, kompresije in novejša znanja o algoritmih
- najbolj uporabljen algoritem je DES (Data Encryption Standard), AES (The Advanced Encryption Standard)

Simetrični sistemi danes

- uporabljeni so v gospodarstvu, bančništvu, vojski...
- izmenjava ključev predstavlja poseben problem pri velikem številu partnerjev in velikih razdaljah
- DES je moč zlomiti:
 - ◆ sep.1998: z uporabo posebne strojne opreme za 250.000 \$ v treh dneh (Datamation, sep. 1998)
 - ◆ jan.2001: v nekaj urah (NetworkMagazine)

Asimetrični sistemi - osnove

Posebni algoritem generira dva ključa:

- zasebnega in
- javnega

Teorija zagotavlja, da se postopka enkripcije in dekripcije lahko izvedeta le z ustreznim parom ključev.

Asimetrični sistemi - hranjenje ključev

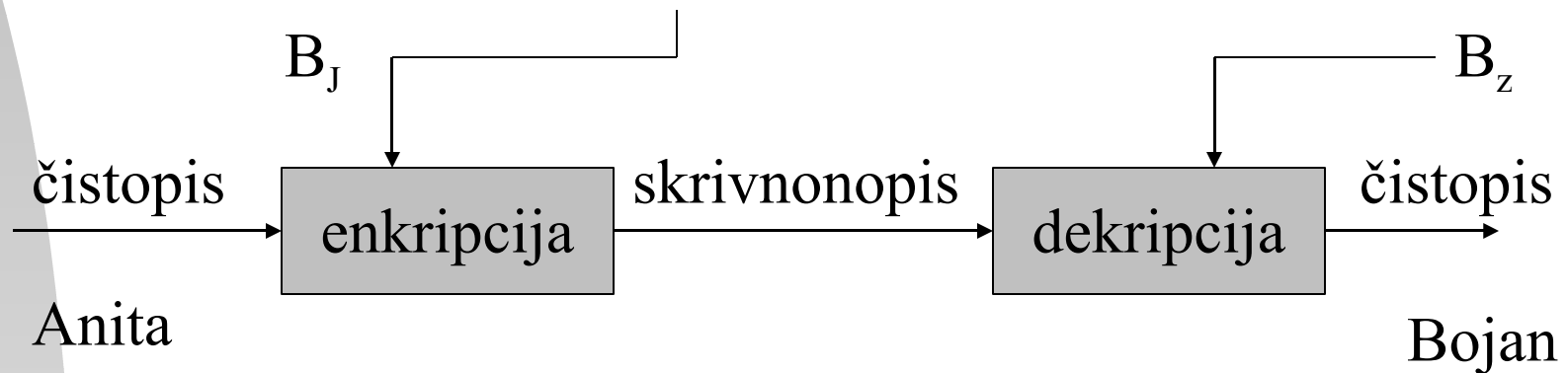
- zasebni ključ pozna le lastnik; hrani ga na varnem mestu (večinoma je varovan tudi z geslom ali PIN), npr.:
 - pametna kartica
 - magnetna kartica
 - disketa ...
- javni ključ je objavljen kjerkoli (www, poslan po pošti, polna funkcionalnost AS pa je zagotovljena le z Infrastrukturo Javnih Ključev - IJK in Certificate Authority – CA – SIGEN-CA v Sloveniji)

Asimetrični sistemi

- temeljijo na celoštevilski algebri (teorija velikih praštevil, diskretni logaritmi)
- tipične dolžine ključev so preko 100 bitov z možnostjo povečevanja
- so računsko zelo zahtevni
- v praksi se uporabljajo za kratka sporočila (digitalni podpis in izmenjavo simetričnega ključa)

AS: zagotavljanje zaupnosti

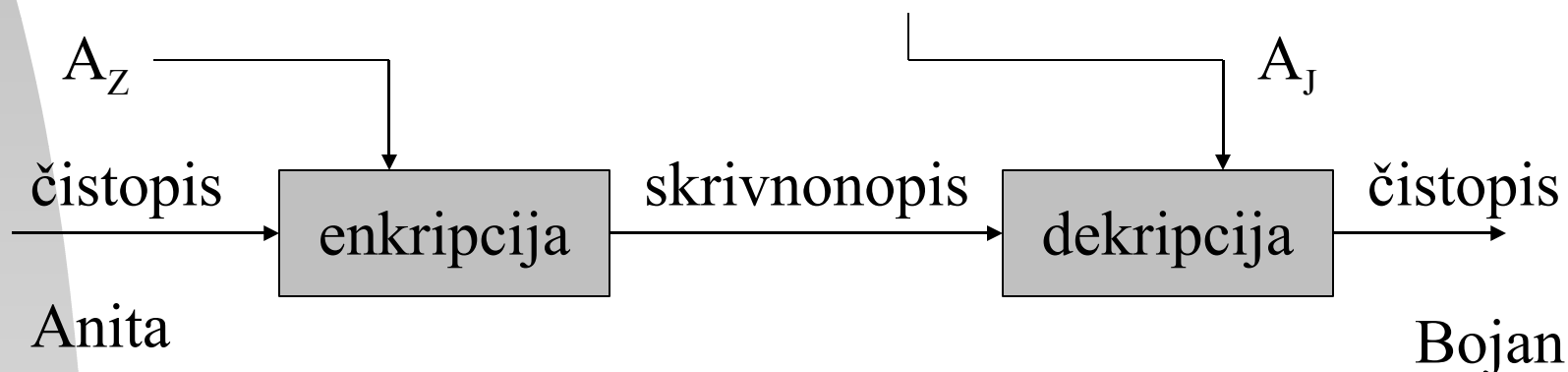
- Anita želi poslati skrivno sporočilo Bojanu: enkriptira ga z njegovim javnim ključem



B_J ... Bojanov javni ključ
 B_Z ... Bojanov zasebni ključ

AS: ugotavljanje verodostojnosti

- Anita želi poslati javno sporočilo Bojanu; Bojan želi biti prepričan o avtorju: Anita enkriptira sporočilo s svojim zasebnim ključem



A_J ... Anitin javni ključ

A_Z ...Anitin zasebni ključ

AS: zaupnost in verodostojn.

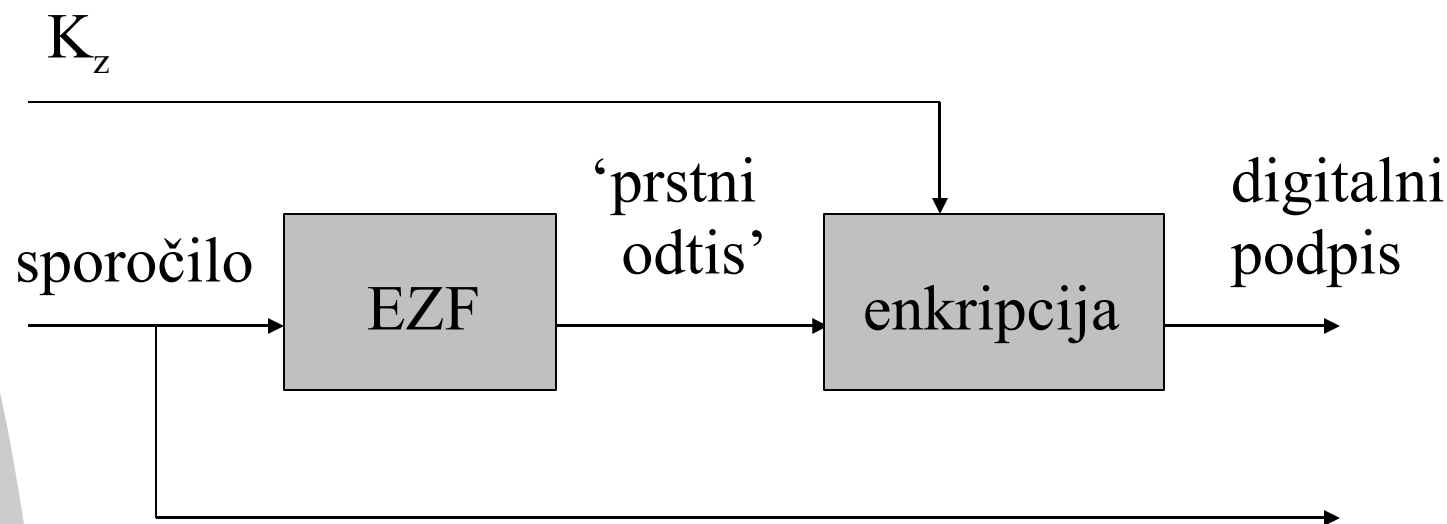
- varianta 1: enkripcijo izvedemo dvakrat: uporabimo naslovnikov javni ključ in nato na rezultatu še svoj zasebni ključ; prejemnik (naslovnik?) naredi ustrezni obratni operaciji
- varianta 2: uporabimo enosmerno zgoščevalno funkcijo in digitalni podpis (overjanje), nato sporočilo enkriptiramo z naslovnikovim javnim ključem (zaupnost)

Enosmerne zgoščevalne funkcije (EZF)

- izdelajo 'prstni odtis' sporočila
- lastnost 1: vsaka sprememba v sporočilu se odraža v vrednosti EZF
- lastnost 2: praktično je nemogoče najti dve različni sporočili z enako vrednostjo EZF



Digitalni podpis - postopek



- hkrati s podpisom se pošlje tudi sporočilo

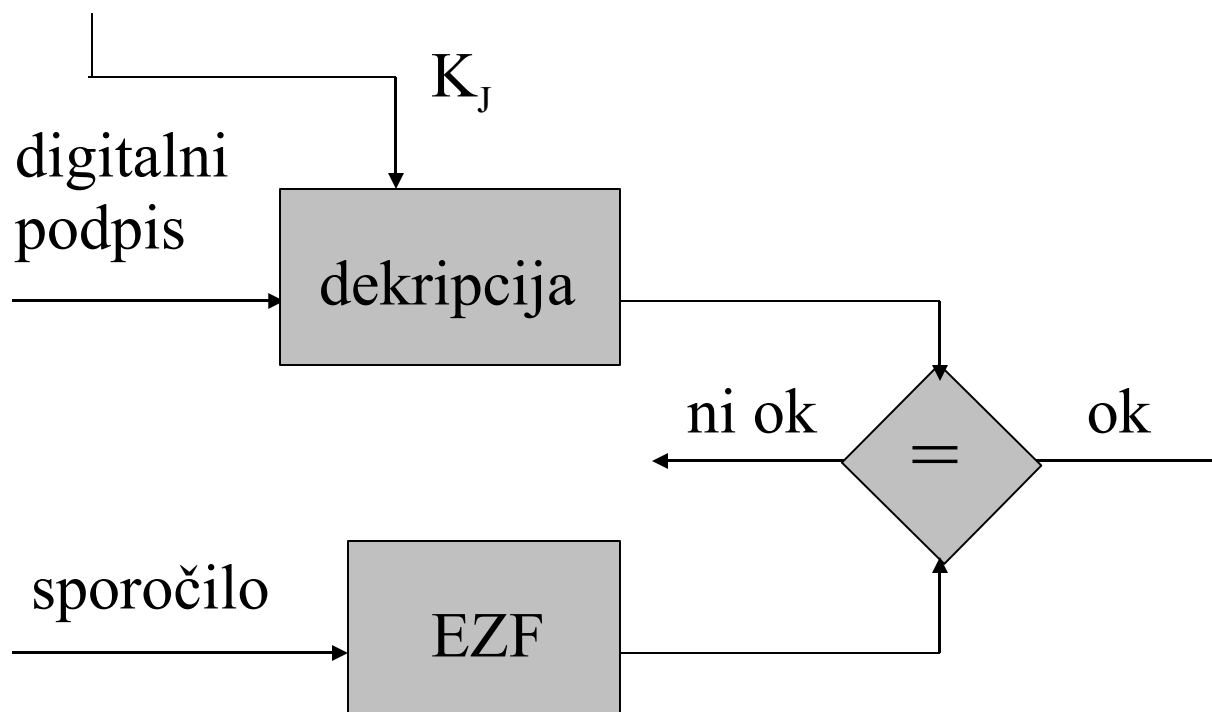
Digitalni podpis

omogoča ugotavljanje celovitosti sporočila, verodostojnosti pošiljatelja in nezatajljivost. Ne zagotavlja zaupnosti.

Prejemnik preveri podpis po naslednjih korakih:

- ◆ dekriptira podpis (uporabi javni ključ)
- ◆ izvede EZF na sporočilu
- ◆ primerja rezultata

Digitalni podpis - preverjanje



Certificate Authority (CA)

(overitelji, agencije za certificiranje javnih ključev)

- osnovni problem ključev pri AS: Kako vemo, da javni ključ res pripada neki osebi?
- *CA je zaupanja vredna organizacija, ki hrani javne ključe in izdaja certifikate*
- CA in uporabnik si ob vzpostavitvi sodelovanja izmenjata svoja javna ključa.

Certifikat

- je potrdilo o ustreznosti javnega ključa
- vsebuje: ime lastnika javnega ključa, njegov javni ključ, čas veljavnosti, čas izdaje...
- podpisan je z skritim ključem CA
- javni ključ lastnika dobimo z dekripcijo z javnim ključem CA
- za učinkovito uporabo AS potrebujemo Infrastrukturo javnih ključev (IJK, tudi varnostna infrastruktura)

Infrastruktura javnih ključev omogoča

kompleksno upravljanje z javnimi ključi, med drugim:

- generiranje
- hranjenje
- porazdeljevanje
- preklicevanje
- certificiranje

Gradniki Infrastrukture Javnih Ključev

- hierarhično povezane CA
- časovna normala (zagotavlja jo NTP)
- podatkovno skladišče
- protokoli za upravljanje s ključi

Primerjava kr. sistemov

	SS	AS
<i>CPU zahtevnost</i>	majhna	zelo velika
<i>število potrebnih ključev narašča</i>	kvadratično *	linearno *
<i>digitalni podpis</i>	ne omogočajo	omogočajo
<i>upravljanje s ključi</i>	zahtevno	pogoj je IJK **

* s številom partnerjev

** za polno funkcionalnost

Dolžina ključev

- daljši ključ načeloma pomeni večjo varnost
- tipične dolžine današnjih ključev: 48, 56, 128... do 1024 bitov (primer: št. sekund v tisoč letih zapišemo z 31 biti $\approx 1,5 \cdot 10^9$)
- Moorov zakon: zmogljivosti računalnikov se podvojijo vsakih 18 mesecev; ključi, ki so pogojno trenutno še varni, kmalu ne bodo
- DES: 56 bitov
- AES: 128, 192 in 256 bitov

Dolžina ključev (nadalj.)

<i>št.bitov</i>	<i>št.ključev</i>	<i>primer</i>
56	$7,2 \times 10^{16}$	DES
128	$3,4 \times 10^{38}$	AES
192	$6,2 \times 10^{57}$	AES
256	1.1×10^{77}	AES

SS in AS danes

- uporabljajo se vsi
- veliko se AS uporabljajo pri vzpostavitvi zveze za izmenjavo simetričnih ključev, izmenjava podatkov pa nato poteka s SS
- za polno funkcionalnost AS potrebujemo Infrastrukturo javnih ključev (IJK), ki pa žal še ni na razpolago, in ustrezno zakonodajo
- ZDA: od pomladi 2001 se DES postopoma nadomešča z AES (Advanced Encryption Standard)

AS jutri

- IJK bo omogočila varno komuniciranje
- uporabljeni ključi bodo vedno daljši
- programska oprema bo omogočala preprostejšo uporabo kriptografije