"PAMETNI" IDENTIFIKATORI (Pametne kartice)

Prof. dr Nedjeljko Lekic

ŠTO SU "PAMETNE" KARTICE?

"Pametne" kartice ili čip katrice ili kartice sa integrisanim kolom (**ICC**).

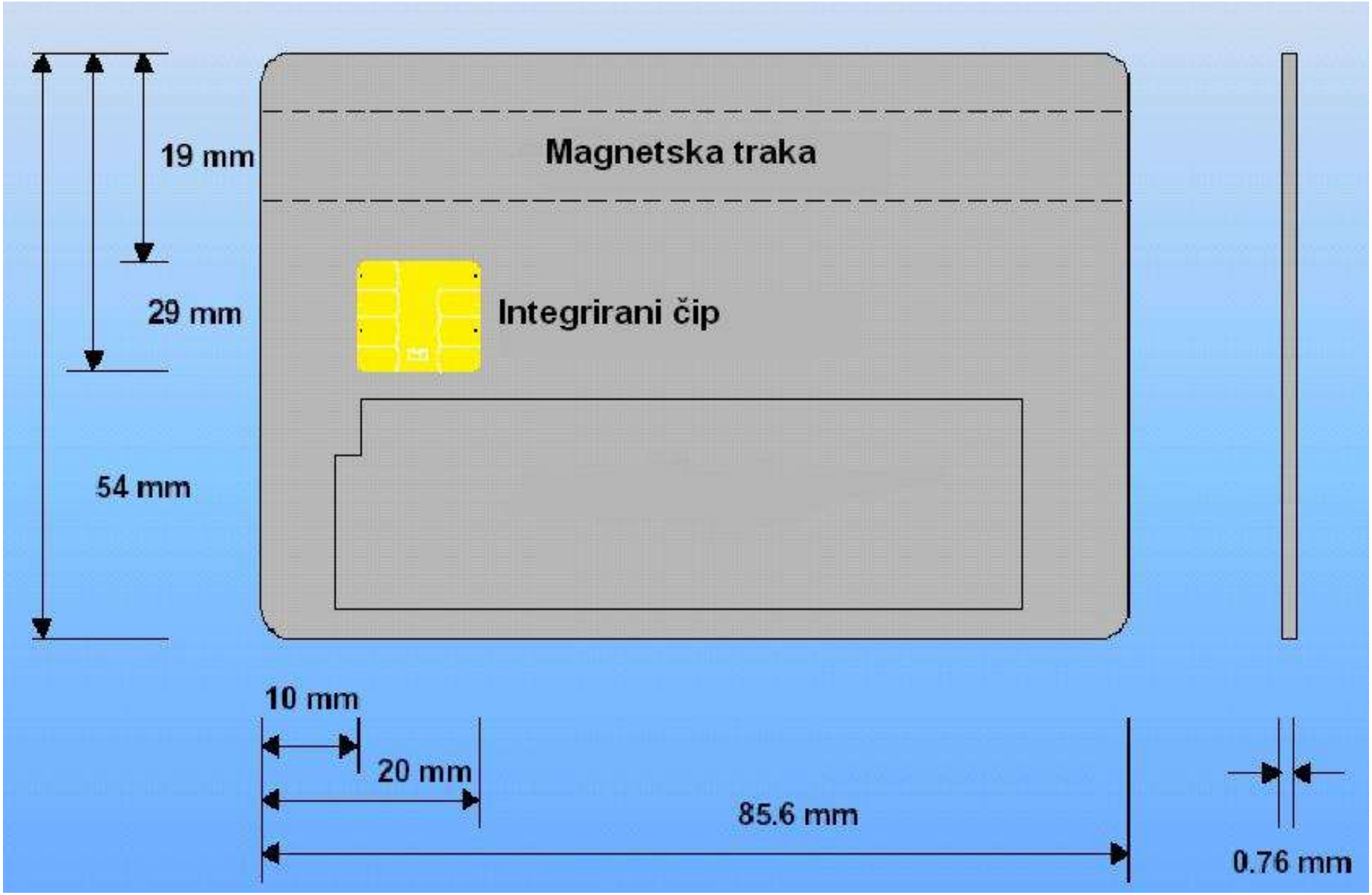
Svaka kartica, standardne veličine, sa ugrađenim integrisanim kolom koje može obrađivati informacije, naziva se "pametna" kartica.

Ovo znači - kartica može primati podatke, procesirati ih i odašiljati.

Siguran nosilac elektronskog identiteta.

Poseban naglasak na sigurnost podataka i brzinu obrade kritpografskih funkcija.

ŠTO SU "PAMETNE" KARTICE?



ISTORIJAT

″Pametne″ kartice su prvi predložili njemečki naučnici Helmut Gröttrup i Jürgen Dethloff in 1968. Patent je prihvaćen 1982.

Roland Moreno 1974. godine predlaže prvi koncept memorijske kartice.

Prva značajnija upotreba ″pametnih″ kartica bila je u Francuskoj 1983 – za bezgotovinsko plaćanje telefonskih razgovora.

1977. godine Michel Ugon, iz Honeywell Bull-a predstavio je prvu ″pametnu″ karticu sa mikroprocesorom.

Druga velika primjena 1992. godine - u sve debitne kartice u Francuskoj ugradjen je čip (Carte Bleue)

ISTORIJAT

Tokom 1990-ih širom Evrope pojavljuju se sistemi u kojima se ″pametne″ kartice koriste kao elektronski novac.

U ovim sistemima podatak o količini novca čuva se na kartici ne na nekom spoljašnjem računu.

Glavnu primjenu ″pametne″ kartice dobijaju, tokom 1990-ih, uvođenjem SIM kartica u mobilnoj telefoniji.

1993. godine MasterCard i VISA prihvataju uvođenje čipa u njihove kreditne i debitne kartice.

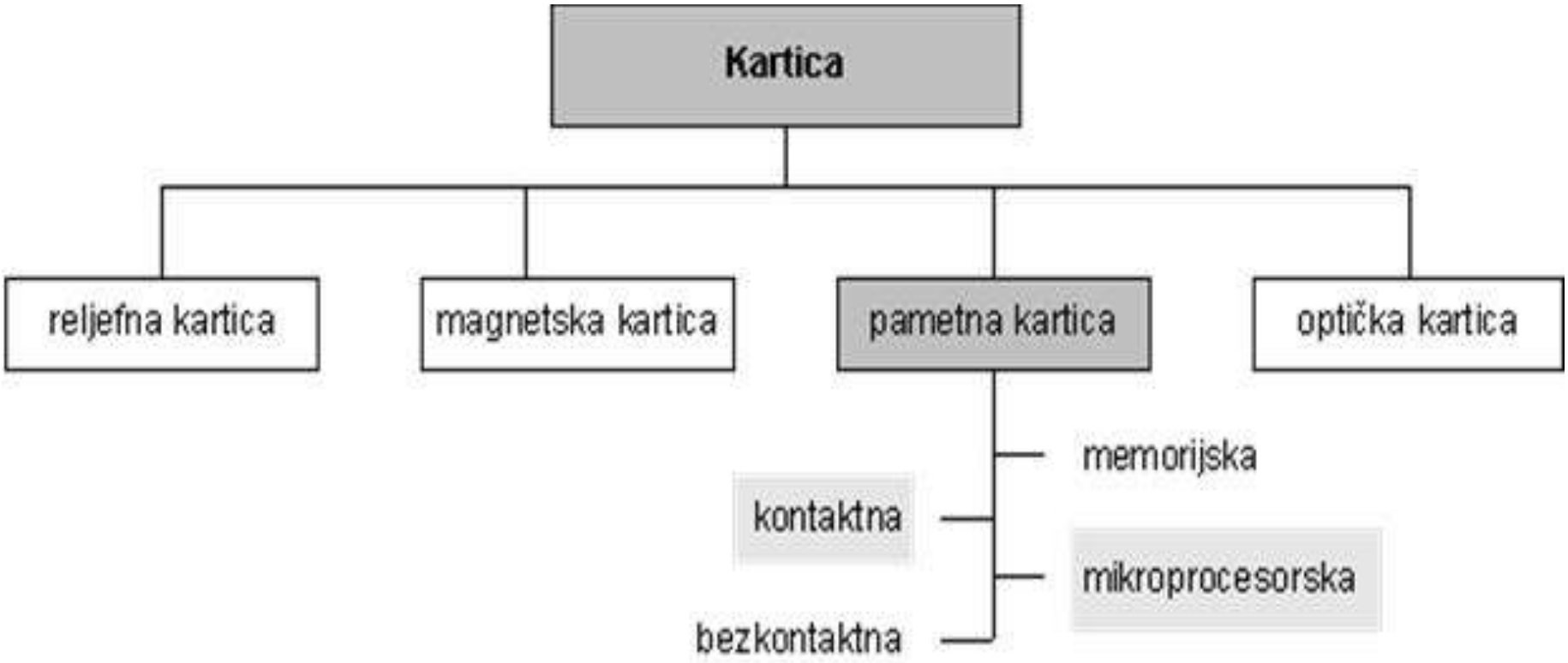
Prva verzija EMV sistema pojavljuje se 1994. godine, zatim 1998, 2000, 2004 …

EMV (Europay, MasterCard and VISA) je standard za upotrebu IC kartice i IC kompatibilnih POS terminala.

Glavni interes banaka za uvođenju pametnih kartice je u smanjenju broja prevara, falsifikovanja i krađa.

Odnos cijena/dobit – USA industrija placanja – bezkontaktne pametne kartice.

TIPOVI KARTICA



Dvostruka provjera prilikom autentifikacije

- **ono što posjeduješ – kartica (identifikator)**
- **ono što znaš - PIN**

VRSTE "PAMETNIH" KARTICA

Sa stanovišta pristupa podacima postoje:

KONTAKTI

- VCC – napajanje
- GND – masa
- RST – reset
- CLK – signal takta
- I/O – ulaz/izlaz
- VPP – prog. napon
- RFU - rezervisano

MEMORIJSKE I MIKROPROCESORSKE

Dvije osnovne kategorije pametnih kartica su:

- Memorijske kartice i
- Mikroprocesorske kartice

Memorijske kartice - sadrže samo postojanu memoriju (EEPROM) i moguće neku specifičnu sigurnosnu logiku.

Mikroporocesorske kartice – sadrže i kratkotrajnu memoriju (RAM) i mikroprocesorske komponente.

Kartice se prave od PVC ili, ponekad, ABS plastike.

U kartici se može ugraditi hologram kao osiguranje od falsifikovanja.

MEMORIJSKE KARTICE

- **Memorijska kartica ima ugrađen čip sa memorijom, ne može se programirati i ne sadrži mikroprocesor.**

- **Omogućen je direktan pristup memoriji i podržava nekoliko naredbi koje se ne mogu mijenjati.**

MEMORIJSKE KARTICE

Na osnovu vrste ugrađene memorije razlikuju se sljedeći tipovi memorijskih kartica:

- ***Kartice sa običnom memorijom***
- ***Kartice sa zaštićenom memorijom***
- ***Kartice sa brojačem***

MEMORIJSKE KARTICE

Kartice sa običnom memorijom

- Namijenjene su uglavnom pohranjivanju podataka.
- Imaju najnižu cijenu po bitu pohranjene informacije.
- Pojavljuju se kao kartice sa čipom i EEPROM memorijom ili kartice sa fleš memorijom.

MEMORIJSKE KARTICE

Kartice sa zaštićenom memorijom

- Imaju ugrađene jednostavne veze za nadzor pristupa podacima.
- Dijeljena memorija – multiaplikativnost.
- Određeni djelovi memorije mogu se zaštiti od pisanja i brisanja, što se obično postiže šiframa ili sistematskim ključevima.
- Upotrebljive su tamo gdje nije neophodna visoka sigurnost podataka.

MEMORIJSKE KARTICE

Kartice sa brojačem

- Namenjene su držanju vrijednosti,
- Za jednokratnu ili višekratnu upotrebu.
- Tipičan primer takvih kartica su telefonske kartice.

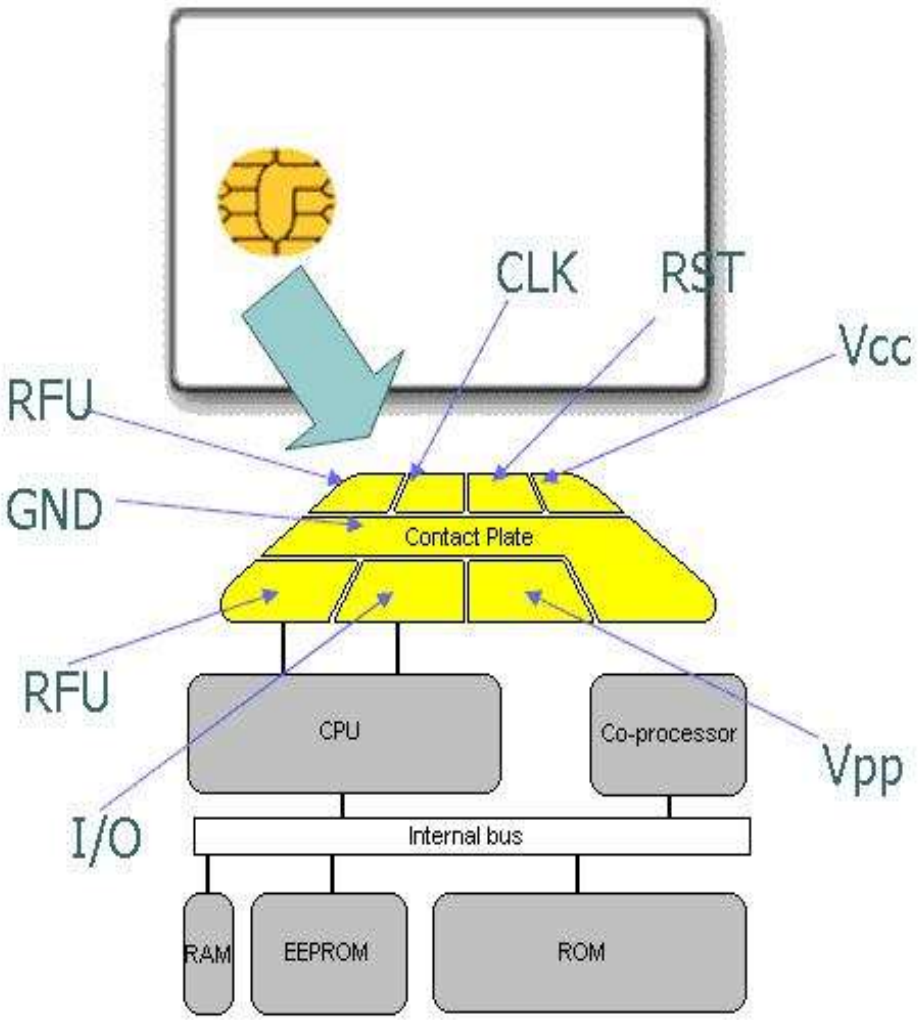
- Usljed jednosmjernog rada brojača telefonska kartica postaje neupotrebljiva nakon što se potroši predefinisani kredit.

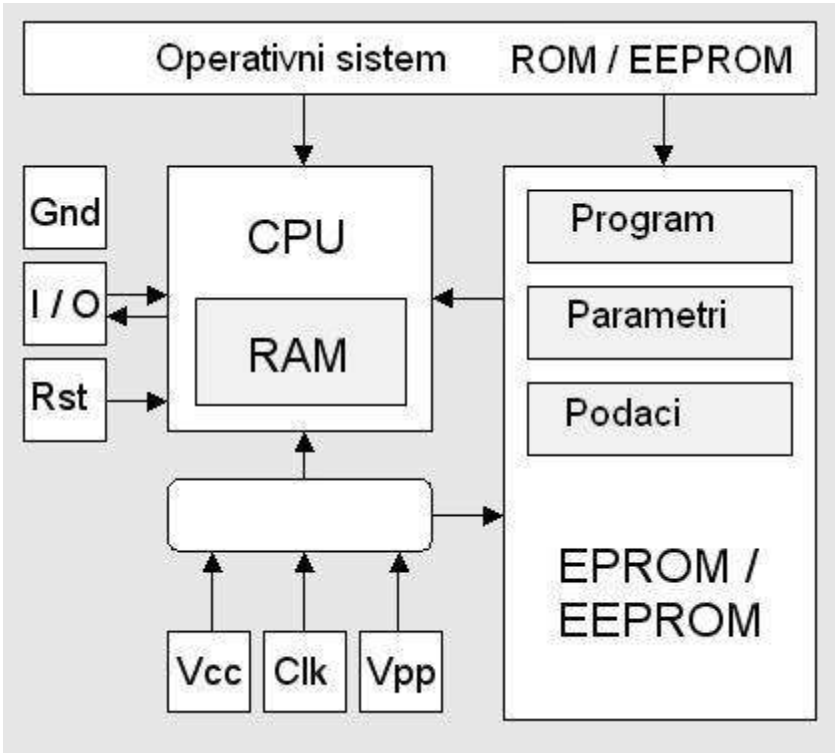
MIKROPROCESORSKE KARTICE

- Kao što i sam naziv govori, mikroprocesorske kartice sadrže mikroprocesor.
- Mikroprocesor značajno podiže sigurnost podataka.
- Sposobne su obrađivati, pamtiti i zaštititi podatke i donositi odluke u određenim granicama.
- Omogućavaju ugradnju kriptografskih algoritama i primjenu širokog skupa zaštitnih mehanizama.
- Često se naziv pametna kartica vezuje samo za mikroprocesorske kartice.

MIKROPROCESORSKE KARTICE

ŠTO JE U KARTICI?





CPU	8bit 5MHz
RAM	256 – 1 kBytes
ROM	4-24 kBytes
EEPROM	1-16 kBytes

MIKROPROCESORSKE KARTICE

Mikroprocesorska kartica - PC u malom. Sadrži:

- ***Procesor*** **(CPU) pomoću koga se vrše izračunavanja,**
- ***Read-Only Memory*** **(ROM), memorija na kojoj se nalazi operativni sistem i aplikativni program,**
- ***Random Access Memory*** **(RAM), memorija koja se koristi za privremeno skladištenje podataka tokom rada procesora,**
- ***Electronically Erasable and Programmable Read-Only Memory*** **(EEPROM), memorija u kojoj su smješteni podaci od interesa (broj tekućeg računa, sertifikati, ključevi i sl.),**
- ***Clock i ulazno izlazni interfejs*** **preko koga se komunicira sa okolinom (čitačem).**

Tipična smart kartica ima 8-bit procesor koji radi na 5MHz, 256 do 1024B RAM-a, 6 do 24KB ROM-a, 1 do 16KB EEPROM-a.

MIKROPROCESORSKE KARTICE

Vlastiti operacioni sistem: JavaCard, MultOS, OSCCA, Smartcard.NET i sl.

- omogućavaju pisanje vlastitih aplikacija koje se izvršavaju u sigurnom okruženju.

Konstruisane za ispunjavanje visokih sigurnosnih standarda

MIKROPROCESORSKE KARTICE

Pametna kartica ≈ PC od prije dvije-tri decenije.

Aplikacije se mogu dodavati i nakon izdavanja pametne kartice.

Operativni sistem štiti aplikacije na kartici od napada (trojans, spyware,...)

- Aplikacija se može upisati u karticu samo uz dozvolu izdavača kartice

- Aplikacije su odvojene jedna od druge. Podaci jedne aplikacije su zaštićeni od uticaja druge aplikacije.

- Obezbjeđuje da se proces upisivanja aplikacije izvodi na siguran način.

Aplikacije treba da sadrže mjere zaštite ličnih podataka i ključeva.

SIGURNOST

- Vrlo visok stepen sigurnosti
  - Ugrađeni procesor obavlja enkripciju/dekripciju podataka
  - Povjerljivi podaci ne izlaze iz kartice

- Algoritmi:
  - Simetrično šifrovanje
  - Asimetrično šifrovanje
    - Digitalni potpis

ŠIFROVANJE (ENCRYPTION)

Magična cifra

Promjena je linarna i jednaka za svaku cifru- 3

I agree ⇒ lcdjuhh

i+3=l

Space=c [+3]

Ključ – Niz magičnih cifara

Promjena je linerno (ciklična): 269

k.n.gupta 62 ⇒ mewam3rzjba

k+2=m

(dot)=e [+6]

n=w [+9]

Char	1	2	3	4	5	6	7	8	9
a	b	c	d	e	f	g	h	i	j
b	c	d	e	f	g	h	i	j	k
c	d	e	f	g	h	i	j	k	l
d	e	f	g	h	i	j	k	l	m
e	f	g	h	i	j	k	l	m	n
f	g	h	i	j	k	l	m	n	o
g	h	i	j	k	l	m	n	o	p
h	i	j	k	l	m	n	o	p	q
i	j	k	l	m	n	o	p	q	r
j	k	l	m	n	o	p	q	r	s
k	l	m	n	o	p	q	r	s	t
l	m	n	o	p	q	r	s	t	u
m	n	o	p	q	r	s	t	u	v
n	o	p	q	r	s	t	u	v	w
o	p	q	r	s	t	u	v	w	x
p	q	r	s	t	u	v	w	x	y
q	r	s	t	u	v	w	x	y	z
r	s	t	u	v	w	x	y	z	0
s	t	u	v	w	x	y	z	0	1
t	u	v	w	x	y	z	0	1	2
u	v	w	x	y	z	0	1	2	3
v	w	x	y	z	0	1	2	3	4
w	x	y	z	0	1	2	3	4	5
x	y	z	0	1	2	3	4	5	6
y	z	0	1	2	3	4	5	6	7
z	0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	.
2	3	4	5	6	7	8	9	.	
3	4	5	6	7	8	9	.		a
4	5	6	7	8	9	.		a	b
5	6	7	8	9	.		a	b	c
6	7	8	9	.		a	b	c	d
7	8	9	.		a	b	c	d	e
8	9	.		a	b	c	d	e	f
9	.		a	b	c	d	e	f	g
. (Dot)		a	b	c	d	e	f	g	h
Space	a	b	c	d	e	f	g	h	i

ŠIFROVANJE (ENCRYPTION)

ŠIFROVANJE

Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 1

9a468943… 49f0b9cab28d755aaa9cd985
71b275bbb0ad… 6931e856ca3e5e569e
dd135285482

Message 2

The Internet knows no… It has redefined time an… computer and telecommunicati… have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

Encrypted Message 2

a520eecb61a770f947ca856cd675463f1c95
…9a2b8d4e6a71f80830c87f5715f5f5933497
8d… 7da0707b48a1138d77ced56feba2b4
67c3… 7dbeb86b854f120606a7ae1ed9…
34f570…
b90…

Isti ključ
SIMETRIČNO

Različiti ključevi
[Par ključeva – Javni i Privatni]
ASIMETRIČNO

DEŠIFROVANJE

Encrypted Message 1

9a46894335be49f0b9cab28d755aaa9cd98571b
275bbb0adb405e6931e856ca3e5e569edd13528
5482

Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 2

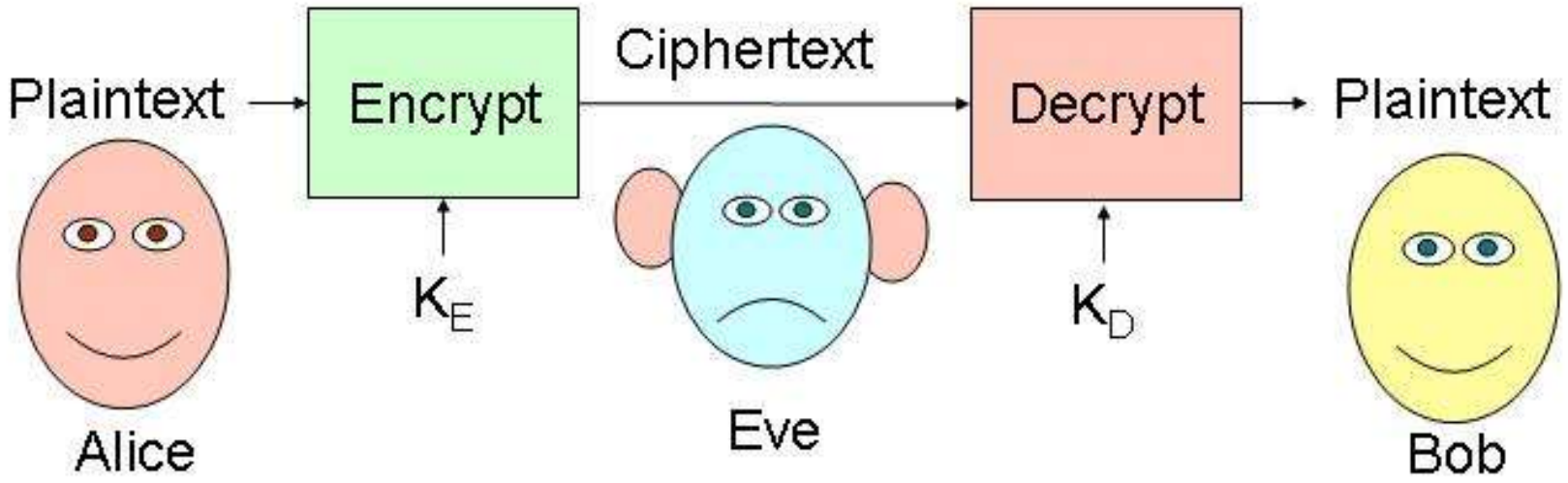
a520eecb61a770f947ca856cd675463f1c95a9a2b
8d4e6a71f80830c87f5715f5f59334978dd7e97da
0707b48a1138d77ced56feba2b467c398683c7db
eb86b854f120606a7ae1ed934f5703672adab0d7
be66dccde1a763c736cb9001d0731d541106f50b
b7e54240c40ba780b7a553bea570b99c9ab3df13
d75f8ccfdddeaaf3a749fd1411

Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

SIMETRIČN0 ŠIFROVANJE

- Šifrovanje tajnim ključem.
- Isti tajni ključ za šifrovanje i dešifrovanje.
- Algoritami šifrovanja su brzi (brži od asimetr. šifrovanja).
- Dobar za kriptovanje velike količine podataka.



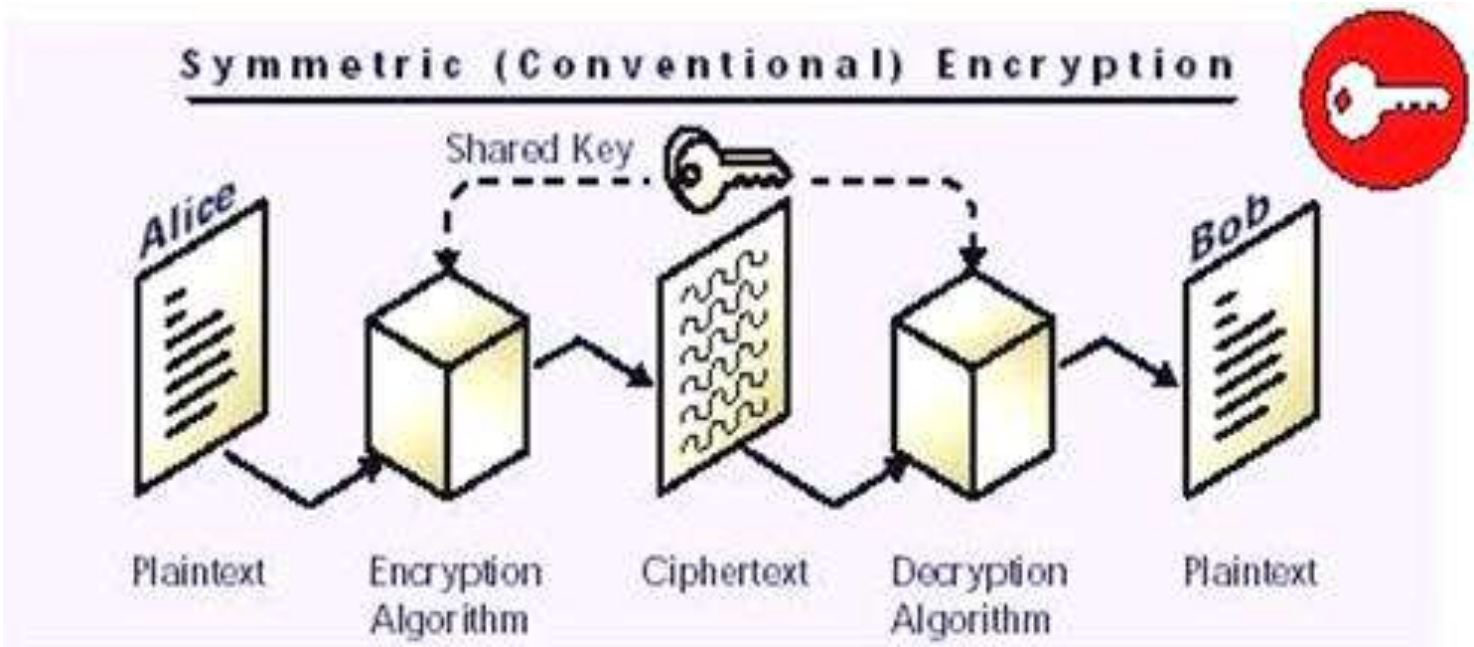
SIMETRIČN0 ŠIFROVANJE

Metod za "razbijanje" ključa: iscrpna pretraga svih mogućih kombinacija za ključ.

Duži ključ – duža pretraga – teže.

Nedostatak – obije komunikacione strane moraju imati isti tajni ključ i isti IV.

Asimetrično kodiranje se koristi za prenos vrijednosti ključa (i **IV**-a).



SIMETRIČN0 ŠIFROVANJE

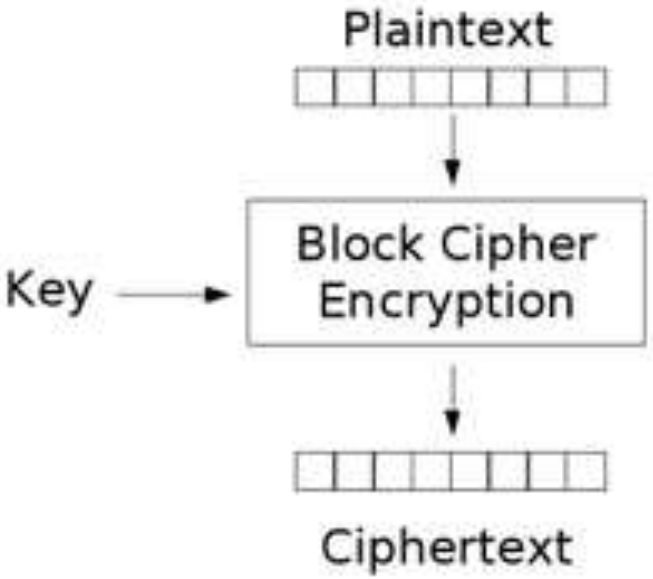
Koriste se tzv. blok algoritmi kriptovanja (Block Chiper Algoritmi - BC): RCS, DES, TripleDES i Rijndael.

BC algoritmi šifrovanjem transformišu ulazni blok od *n* podataka u izlazni blok kriptovanih podataka.

Kriptovanje podataka se vrši blok po blok.

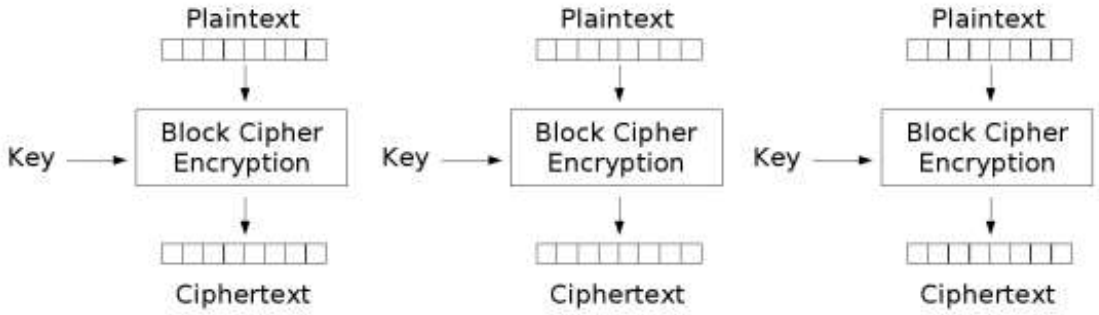
RCS, DES triple i DES: n=8 bytes ,

Rijndeal: n=16 [default] ili 24 ili 32 bytes.

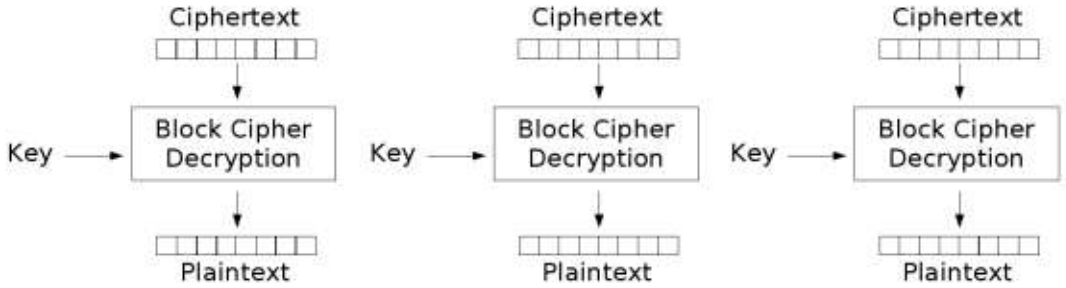


SIMETRIČNO ŠIFROVANJE

Elecetronic Codebook (ECM) način šifrovanja



Electronic Codebook (ECB) mode encryption



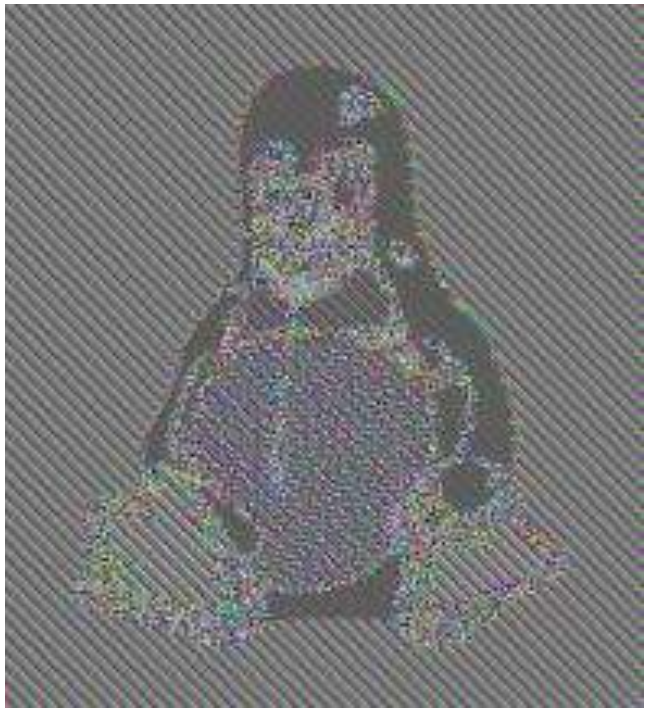
Electronic Codebook (ECB) mode decryption

jednaki blokovi podaka ⇒ jednaki šifr. blokovi

SIMETRIČNO ŠIFROVANJE

Elecetronic Codebook (ECM) način šifrovanja

U nekim slučajevima nedovoljno osiguranje podataka.



SIMETRIČNO ŠIFROVANJE

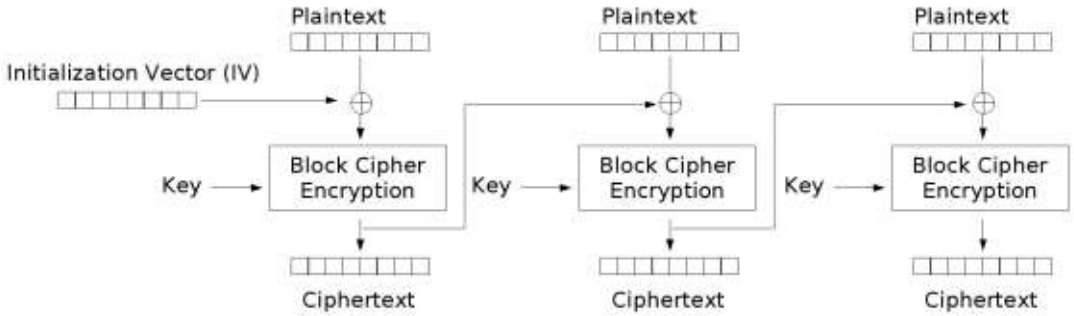
Cipher-block chaining (CBC) način šifrovanja

Lančani mod kriptovanja (Chiper Block Chaining - CBC)

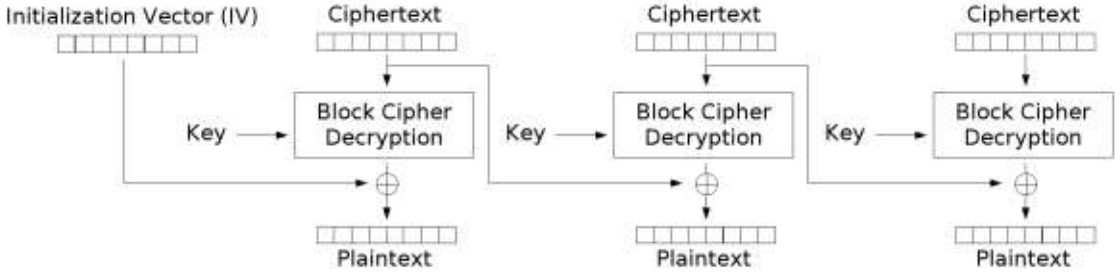
Prethodni blok podataka koristi se za šifrovanje sljedećeg bloka.

IV (inicijalni vektor – blok podataka) šifruje prvi blok podataka.

CBC ⇒ kljuc + IV



Cipher Block Chaining (CBC) mode encryption



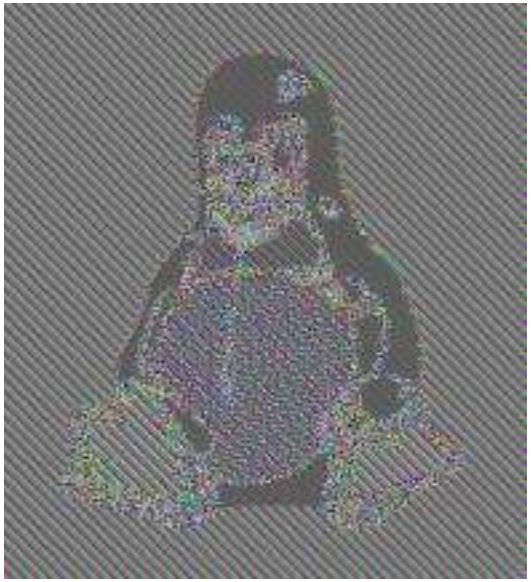
Cipher Block Chaining (CBC) mode decryption

SIMETRIČN0 ŠIFROVANJE

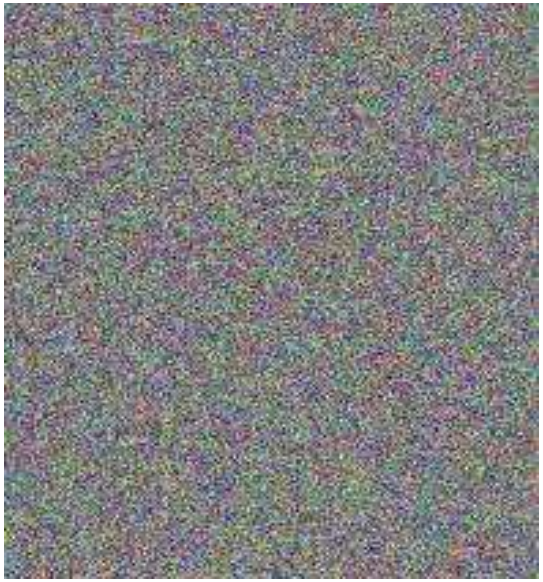
Cipher-block chaining (CBC) način šifrovanja

Bolja zaštita podataka.

Original



ECB mod



CBC mod

STEGANOGRAFIJA (STEGANOGRAPHY)

Steganografija je umjetnost i nauka pisanja skrivenih poruka na način da niko,osim pošiljaoca i primaoca, na posumlja da poruka postoji.

Security through obscurity.

Riječ steganography je grčkog porijekla: *steganos* (στεγανός) znači "prekriven ili zaštićen", i *graphein* (γράφειν) znači "pisati".

SEGANOGRAPHY = SKRIVENO PISANJE

U digitalnoj steganografiji, steganografski kod se može uključiti u document file, media file, program ili protokol.

Media fajlovi su posebno pogodni, zbog svoje veličine.

Jednostavan primjer: pošiljalac može poći od obične slike podestiti boju svakog 100-og pixela tako da odgovara slovu u alphabet-u. Tako mala promjena malo je vjerovatno da će biti primijećena.

STEGANOGRAFIJA (STEGANOGRAPHY)

Slika drveća. Uklanjajući svih osim 2 bita najmanje težine svake kolor komponente, rezultira u gotovo sasvim crnoj slici. Osvjetljavajući takvu sliku 85 puta dobija se slika ispod.

Slika mačke skrivena u slici iznad.

Prednost steganografije, nad kriptografijom, je što poruka ne privlači pažnju.

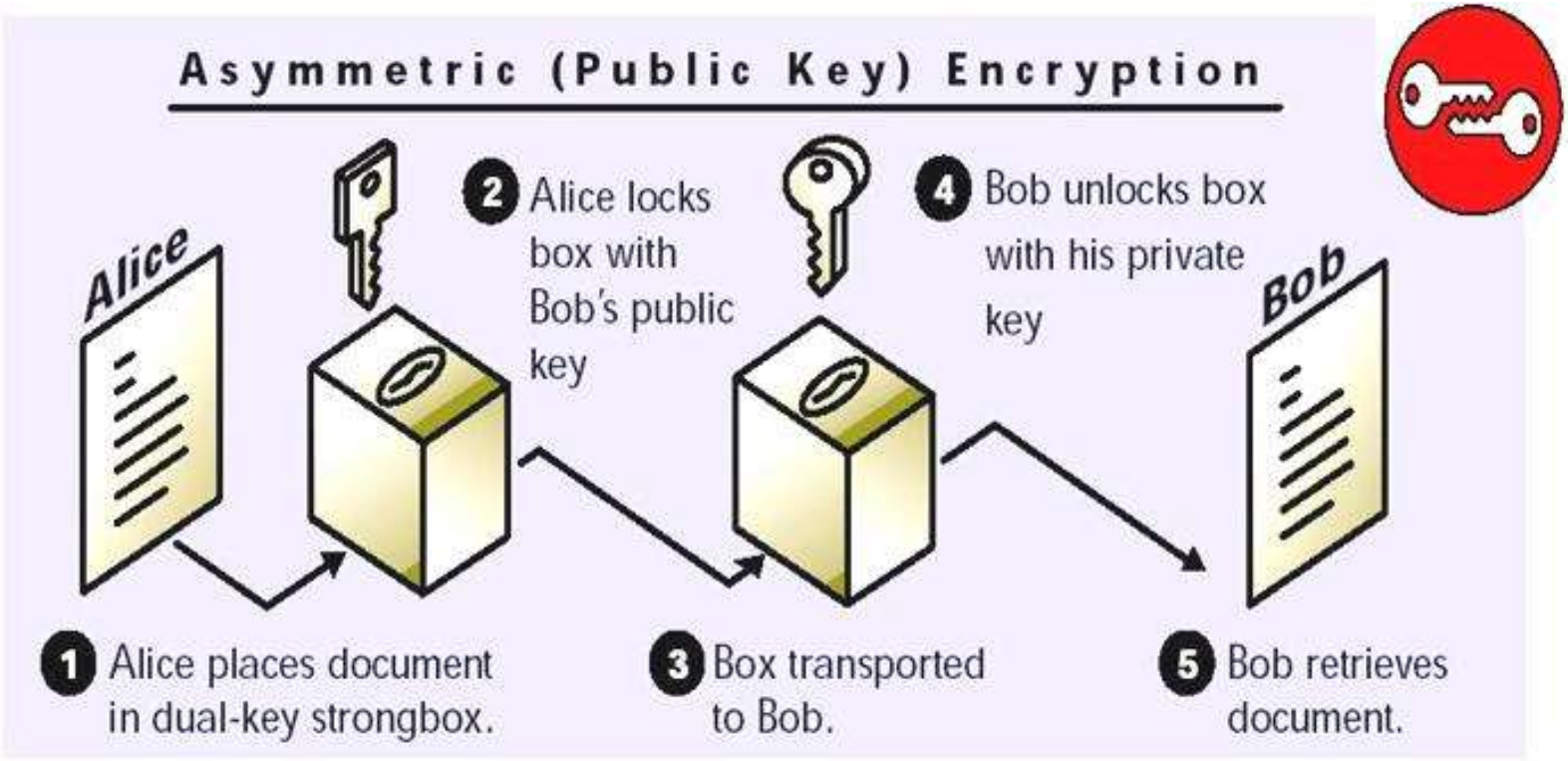
STEGANOGRAFIJA (STEGANOGRAPHY)

Primjer kako teroristi mogu upotrijebiti forumske avatare da pošalju skrivenu poruku.

Ovaj avatar sadrži poruku: "Boss said that we should blow up the bridge at midnight."
šifrovano sa http://mozaiq.org/encrypt upotrebom "växjö" kao lozinke.

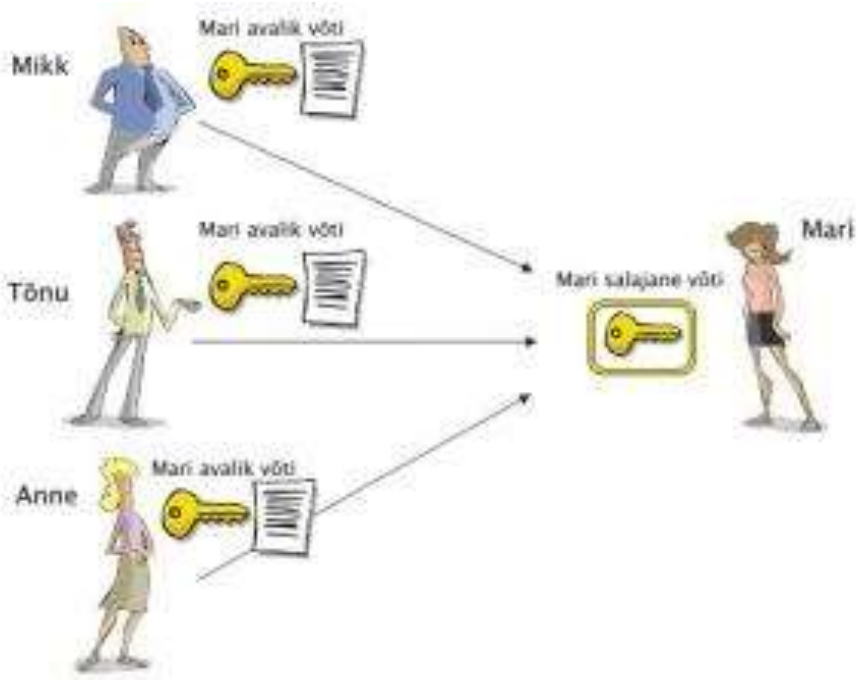
ASIMETRIČNO ŠIFROVANJE

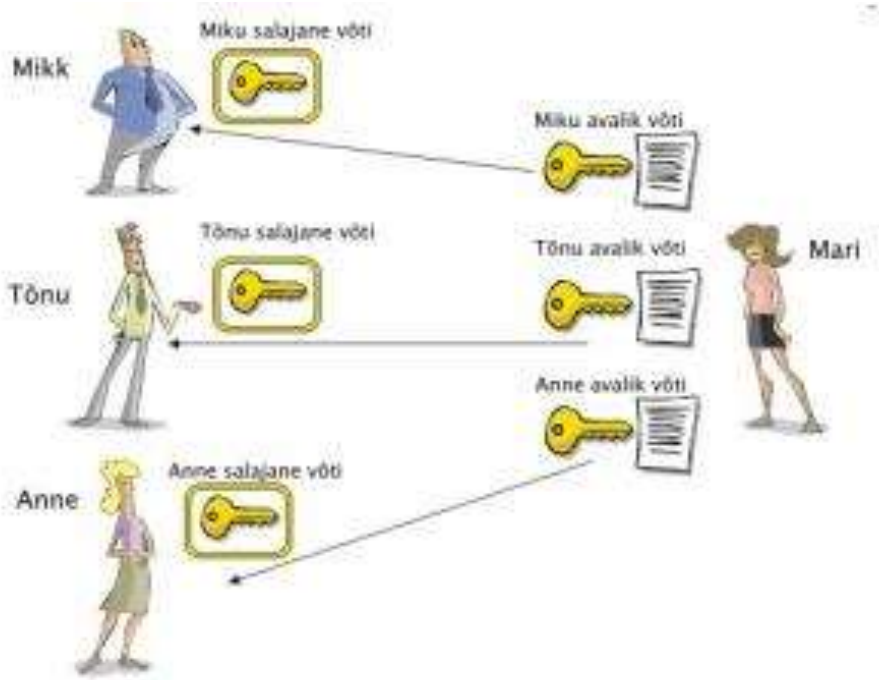
- RSA (Rivest, Shamir i Adleman) algoritmi
- Različiti ključevi za šifrovanje i dešifrovanje.
- Javni i privatni ključ – matematički povezani.



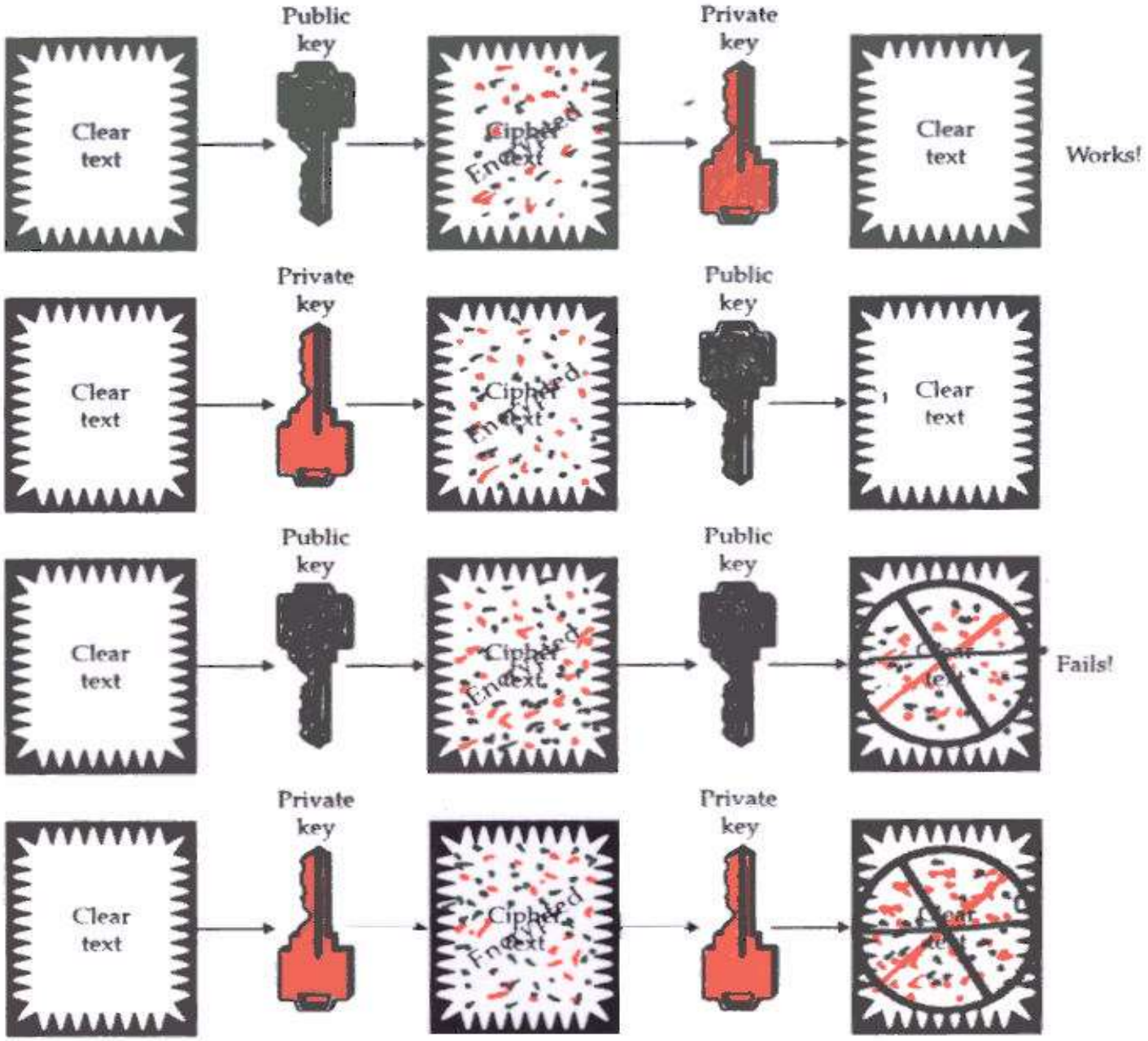
ASIMETRIČNO ŠIFROVANJE

- Veća dužina ključa - sigurnost veća.
- Znatno sporije nego simetrično šifrovanje.
- Za šifrovanje manje količine podataka.
- Često se koristi za kriptovanje tajnog ključa i IV-a, i kao digitalni potpis.





ASIMETRIČNO ŠIFROVANJE



ASIMETRIČNO ŠIFROVANJE - KONCEPTI

1

- 1024-bitni broj je veoma veliki broj, mnogo veći nego ukupan broj elektrona u čitavom svijetu.
- U ovom opsegu postoje trilioni i trilioni parova brojeva koji imaju sljedeću osobinu:
  - Svaka poruka šifrovana sa jednim brojem iz para, može biti dešifrovana JEDINO sa drugim brojem iz istog para brojeva.
- Dva broja iz para nazivaju se ključevi: Javni ključ i Privatni ključ. Korisnik, na svom kompjuteru, generiše vlastiti par ključeva.

2

- Svaka poruka, nezavisno od njene dužine, može se na jedinstven način, komprimovati ili sabiti u poruku manje dužine, koja se naziva izvod (Digest) ili smješa (Hash).
- Najmanja promjena u poruci promijeniće Hash vrijednost (vrijednost izvoda).

ASIMETRIČNO ŠIFROVANJE - KONCEPTI

Svaki pojedinac generiše vlastiti par ključeva

[Javni ključ - poznat svima & Tajni ključ - poznat samo korisniku]

Tajni ključ – Koristi se za šifrovanje poruke
(ili šifrovanje izvoda)

Javni ključ – Koristi se za dešifrovanje poruke
(ili provjeru izvoda)

RSA PAR KLJUČEVA

(uključujući identifikator algoritma)

Privatni ključ

```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2
0d83 463d e493 bab6 06d3 0d59 bd3e c1ce 4367 018a 21a8 efbc
ccd0 a2cc b055 9653 8466 0500 da44 4980 d854 0aa5 2586 94ed
6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1
463d 1ef0 b92c 345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7
8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd e6b7 a991
942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b2f0 1cd5 5ffb
6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16
6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629
4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a
54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04e3 459e a146 2840
8102 0301 0001
```

Javni ključ

```
3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2
0d83 463d e493 bab6 0673 0d59 bf3e c1ce 4367 012a 11a8 efbc
ccd0 a2cc b055 9653 8466 0500 da44 4980 d8b4 0aa5 2586 94ed
6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1
463d 1df0 b92c 345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7
8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd e6b7 a991
942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b250 1cd5 5ffb
6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16
6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629
4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a
54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04de 45de af46 2240
8410 02f1 0001
```

RSA ALGORITAM

Prvi algoritam asimetričnog kriptovanja.

Široka upotreba u eCommerce

Dobio ime po tvorcima Ron Rivestu, Adi Shamiru i Len Adelmanu koji su ga predložili 1977. godine.

Može se koristiti za kriptovanje i za digitalne potpise.

Sigurnost je zasnovana na proračunski zahtjevnom faktoriziranju velikih cijelih brojeva (brojevi veći od 10^{100}).

RSA ALGORITAM

Osnovni koncept RSA algoritma:

1. Odabiraju se dva velika prosta broja p i q. Brojevi trebaju biti približno jednako veliki.
2. U drugom koraku se računa: $n=p \cdot q$.
3. U trećem koraku se računa Euler totient za pq: $\varphi(n)=(p-1)(q-1)$.
4. Odabira se prirodan broj e takav da je $1<e<\varphi(n)$, i da je NZD($\varphi(n)$, e)=1.
5. Izračunava se d takav da je $\boldsymbol{d \cdot e}$ mod ($\boldsymbol{\varphi(n)}$) =1.

   - $de-1$ je djeljiv bez ostatka sa $\varphi(n)$.

   - d predstavlja ekponent tajnog ključa.

Par (n, e) predstavlja javni ključ, dok par (n, d) predstavlja tajni ključ.

RSA ALGORITAM

ŠIFROVANJE

Kada Bob želi poslati poruku M do Alice radi sljedeće:

Poruku podijeli na niz cijelih brojeva jednake dužine $M=m_0m_1m_2m_3...$

Dobijene brojeve šifruje formulom

$$c_i = m_i^e \bmod n$$

DEŠIFROVANJE

Na prijemnoj strani Alice dešifruje poruku primjenom formule

$$m_i = c_i^d \bmod n$$

RSA ALGORITAM

Primjer:

1. Izaberimo proste brojeve p=61 i q=53.
2. Izračunajmo $n=pq$=3233.
3. $\varphi(n)=(p-1)(q-1)$=3120.
4. Izaberimo e >1 a manje od $\varphi(n)$, koje sa $\varphi(n)$ nema zajedniči djelilac.

   Npr. e=17.
5. Odredimo d tako da važi $de \bmod \varphi(n) = 1$. Izračunavanjem se dobija d=2753.

Javni ključ je (n=3233, e=17).

Tajni ključ je (n=3233, d=2753).

Kriptovanjem poruke m=123 dobija se $C=m^e \bmod n = 855$.

Dekriptovanjem slijedi $C^d \bmod n = 123 = m$

ŠTO JE DIGITALNI POTPIS?

- Hash vrijednost (izvod) poruke šifrovana pomoću privatnog ključa osobe, je digitalni potpis na tu poruku.
  - **Digitalni potpis je različit od dokumenta do dokumenta i obezbjeđuje autentičnost svake riječi u dokumentu.**
  - **Kako je javni ključ potpisnika poznat, svako može verifikovati poruku na osnovu digitalnog potpisa.**

DIGITALNI POTPIS

I agree

efcc61c1c03db8d8ea8569545c073c814a0ed755

My place of birth is at Gwalior.

fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25

I am 62 years old.

0e6d7d56c4520756f59235b6ae981cdb5f9820a0

I am an Engineer.

ea0ae29b3b2c20fc018aaca45c3746a057b893e7

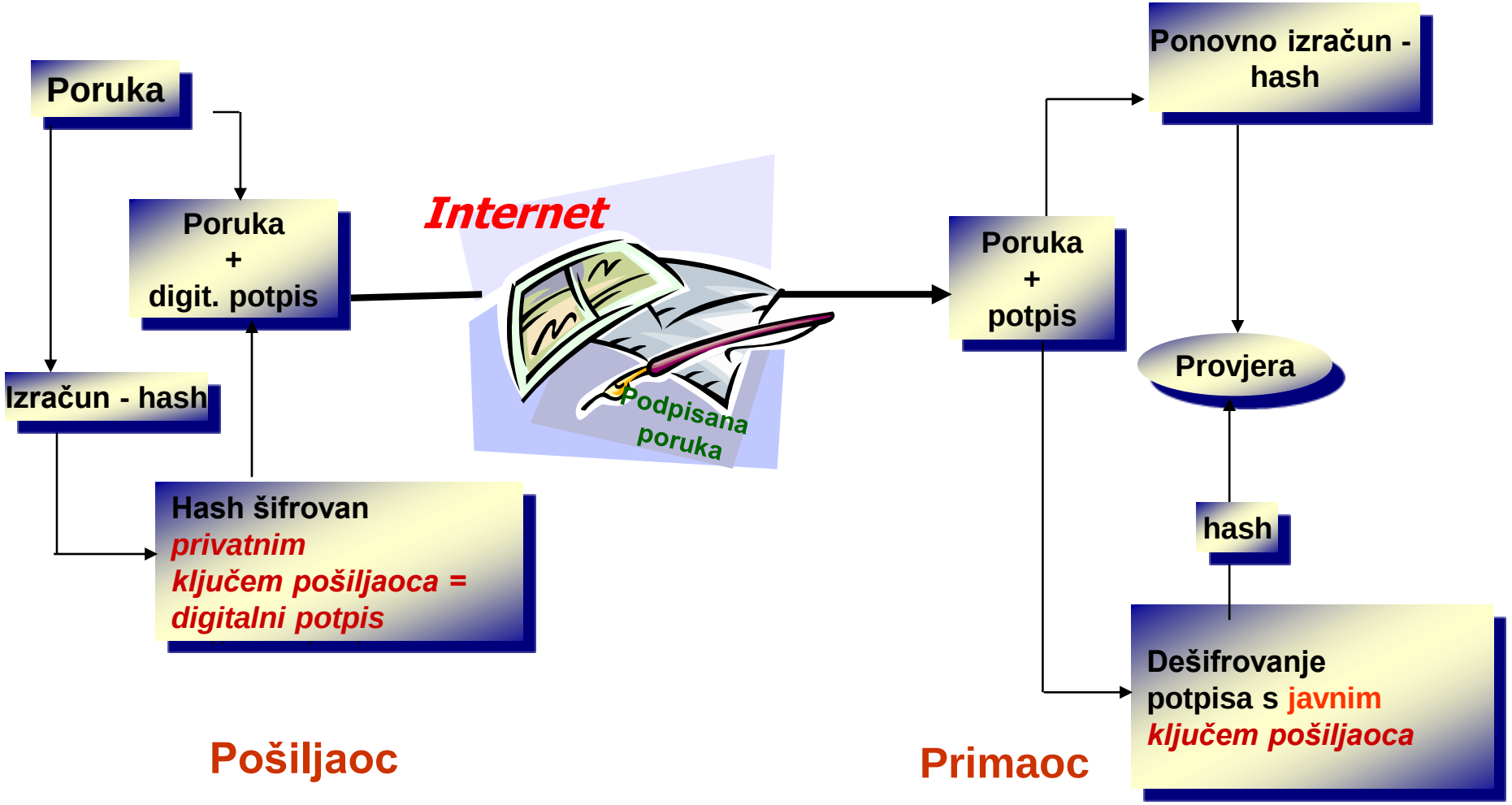
I am a Engineer.

01f1d8abd9c2e6130870842055d97d315dff1ea3

- Ovo su digitalni potpisi iste osobe na različitim dokumentima.

- Digitalni potpis predstavljen heksadecimalnim ciframa.
- Zavisan je od sadržine dokumenta.

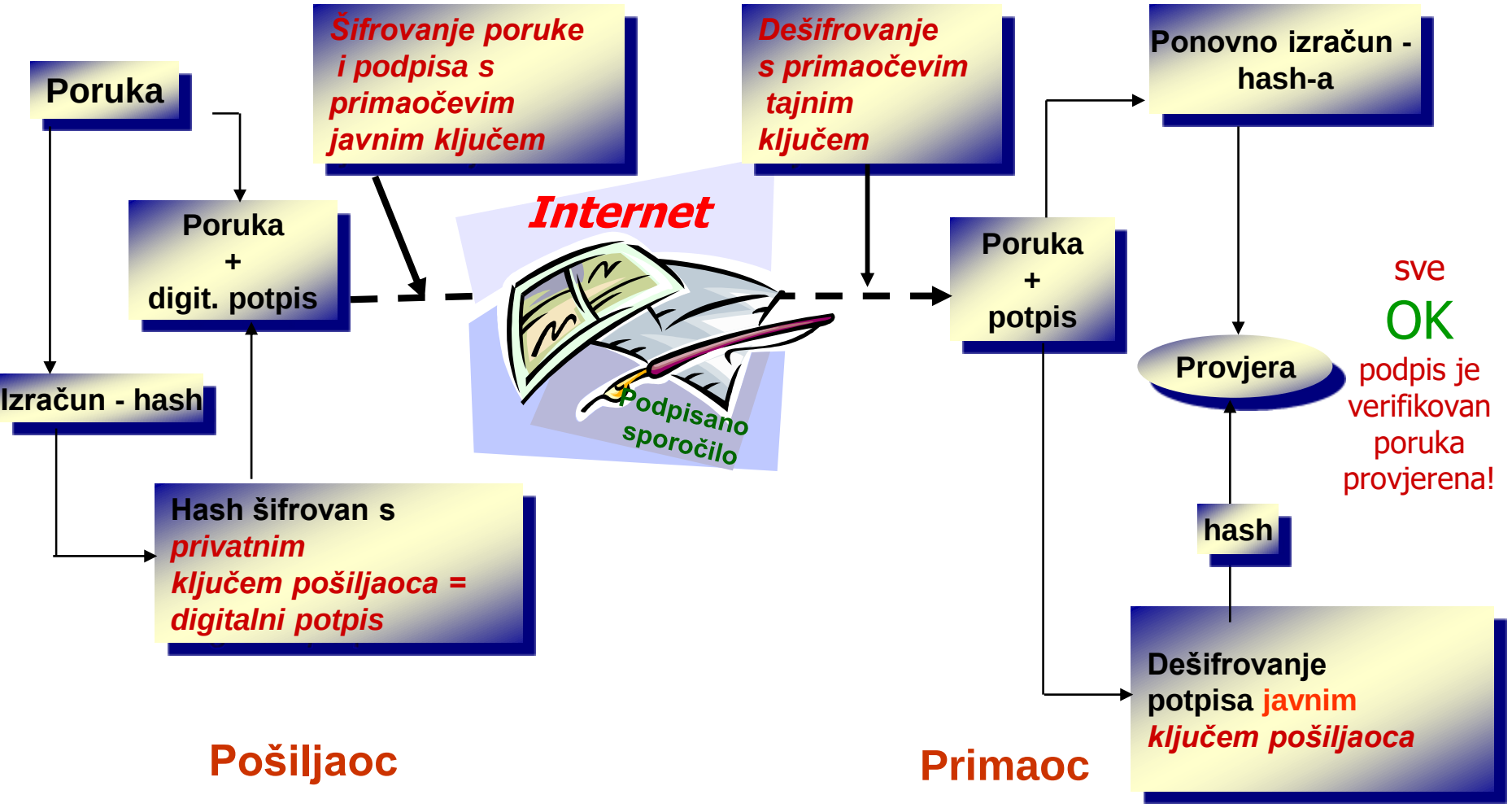
POTPISANA PORUKA



Ovime je osigurana autentičnost i cjelovitost poruke.

Što je sa **tajnošću** poruke?

POTPISANA I ŠIFROVANA PORUKA



Šifrovanje poruke i digitalnog podpisa s primaočevim javnim ključem osigurava tajnost prenosa.

RUČNI POTPIS v/s DIGITALNI POTPIS

Parametar	Papir	Elektronika
Autentičnost	Može se krivotvoriti	Ne može se kopirati
Integritet	Potpis nezavistan od dokumenta	Potpis zavisi od sadržine dokumenta
Prihvatanje-odbacivanja	a. Potreban ekspert za rukopise b. Moguća greška	a. Svaki kompjuter b. Bez greške

ZAŠTITA PRIVATNOG KLJUČA

- Privatni ključ se mora čuvati u tajnosti.
- **Načini čuvanja:**
  - **Ključ na disku – zaštićen PIN kodom**
  - **"Pametne" kartice**
  - **Hardverski ključ (iKey)**

PRIVATNI KLJUČ ZAŠTIĆEN PIN KODOM

- Privatni ključ je šifrovan i čuva se na hard disku u fajlu. Fajl je zaštićen lozinkom.
- Ovo je najnesigurniji način čuvanja privatnog ključa jer
  - Ključ je dostupan.
  - lozinka se može saznati ili "razbiti".

PRIVATNI KLJUČ I "PAMETNE" KARTICE

- Privatni ključ se generiše u kripto modulu kartice i ostaje u "pametnoj" kartici.
- Ključ se čuva u memoriji pametne kartice.
- Ključ je veoma bezbjedan jer ne napušta karticu. Poruka se šalje kartici na potpis i potpis napušta karticu.
- Kartica obezbjeđuje prenosivist ključa pa se potpisivanje (šifrovanje) može vršiti bilo gdje.

  (Gdje postoji čitač kartica)

PRIVATNI KLJUČ I iKey

- Funkcionalnost slična "pametnoj" kartici
  - Ključ se definiše unutar iKey-a.
  - Ključ ne napušta iKey.
  - Prenosivost.
  - Ne zavisi od mašine.
- Prednost iKEY je što ne zahtijeva specijalni čitač. Može se povezati u sistem preko USB porta.

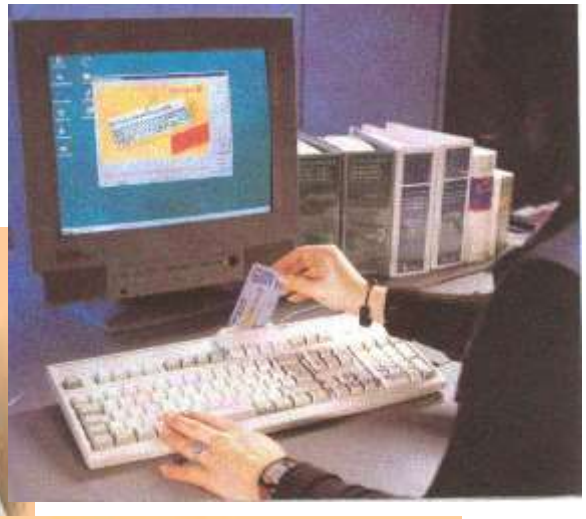
BIOMETRIJA I PRIVATNI KLJUČ

"Pametna" kartica

iKey

Biometrijski podaci – podižu nivo sigurnosti privatnog ključa.

BIOMETRIJA I PRIVATNI KLJUČ



INFRASTRUKTURA JAVNIH KLJUČEVA

- Potrebna je zastupna organizacija, koja potvrđuje vezu između korisnika i njegovog javnog ključa. To je "digitalni notar" ili

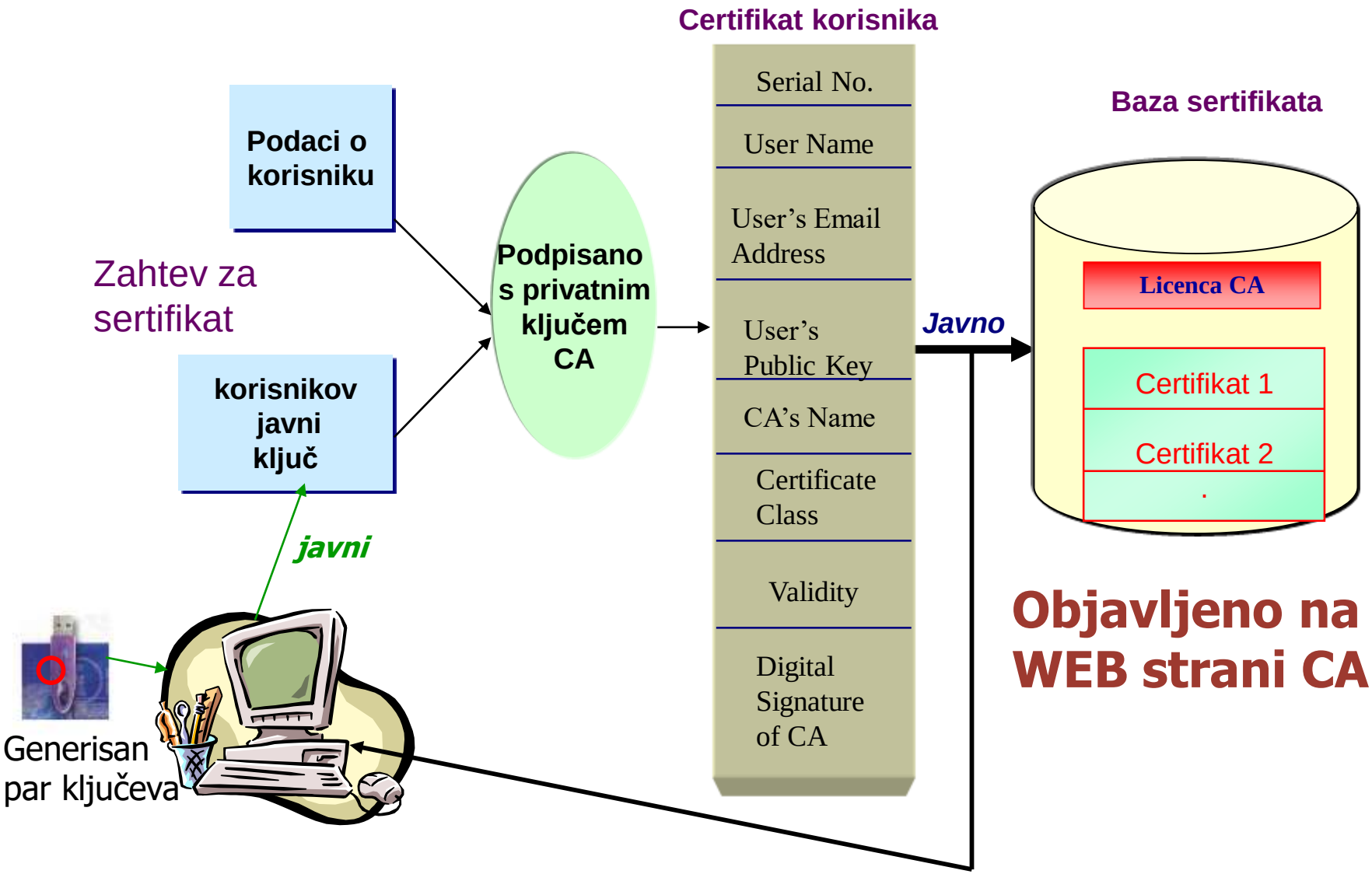
  Certifying Authority (CA) – ustanova za ovjeravanja - ovjeritelj

  Elektronski certifikat potvrdjuje povezanost javnog ključa i korisnika.
- Sve elektronske certifikate elektronski podpisuje CA!

USTANOVA ZA OVJERAVANJA (CA)

- Mora biti javna i povjerljiva
- Mora imati precizno definisan postupak za izdavanje sertifikata.
- Stalan pristup izdatim sertifikatima.
- Stalan pristup ukinutim sertifikatima.
- Stalan pristup licenci dobijenoj od strane nadzornog organa (kontrolera).
- Izvještaj o procesu ovjeravanja (CPS) stalno dostupan na Web-u.
- Striktno poštovanje propisane regulative i uputstava.

INFRASTRUKTURA JAVNIH KLJUČEVA



INFRASTRUKTURA JAVNIH KLJUČEVA

CA privatni ključ zahtijeva najviši nivo sigurnosti.

Hardware Security Module (HSM) koristi se za čuvanje privatnog ključa.

Više od jedne osobe je potrebno za potpisivanje.

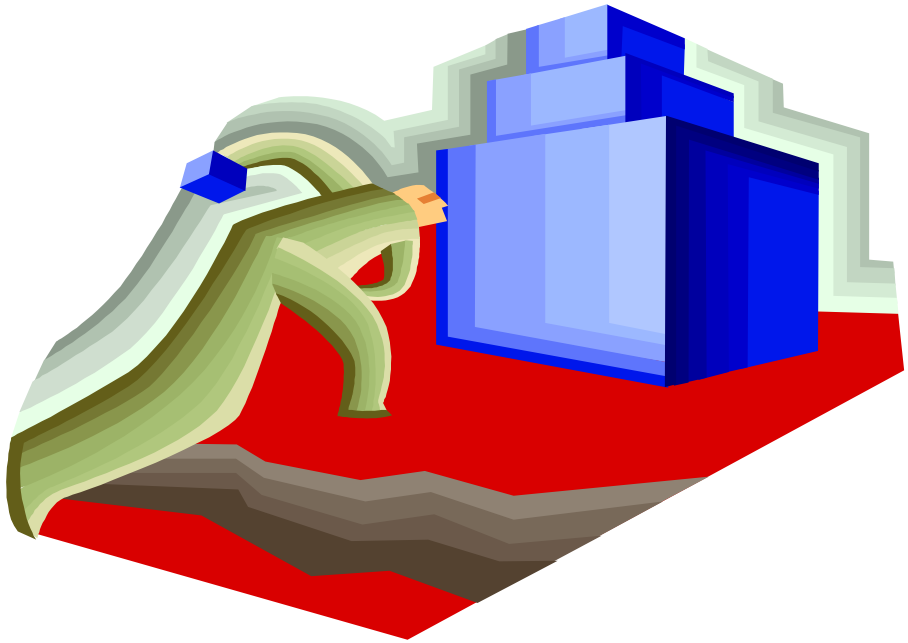
HSM je smješten u strogo čuvanoj prostoriji sa video nadzorom 24 sati dnevno, 7 dana nedjeljno.

POUZDAN PUT

- Nadzorni organ (Controller) je odgovoran za rad ustanova za ovjeravanje (CA)
- Nadzorni organ ovjerava povezanost CA sa CA javnim ključem
- Ustanova za ovjeravanje (CA) je povjerljiv autoritet odgovoran za kreiranje i ovjeru identiteta.
- CA ovjerava povezanost individue sa svojim javnim ključem.

ULOGA NADZORNOG ORGANA

Organ koji nadzire ustanove za ovjeravanje, kao jezgro sistema ovjerava tehnologije, infrastrukturu i djelovanje CA licenciranih za ovjeravanje identiteta.



REZIME

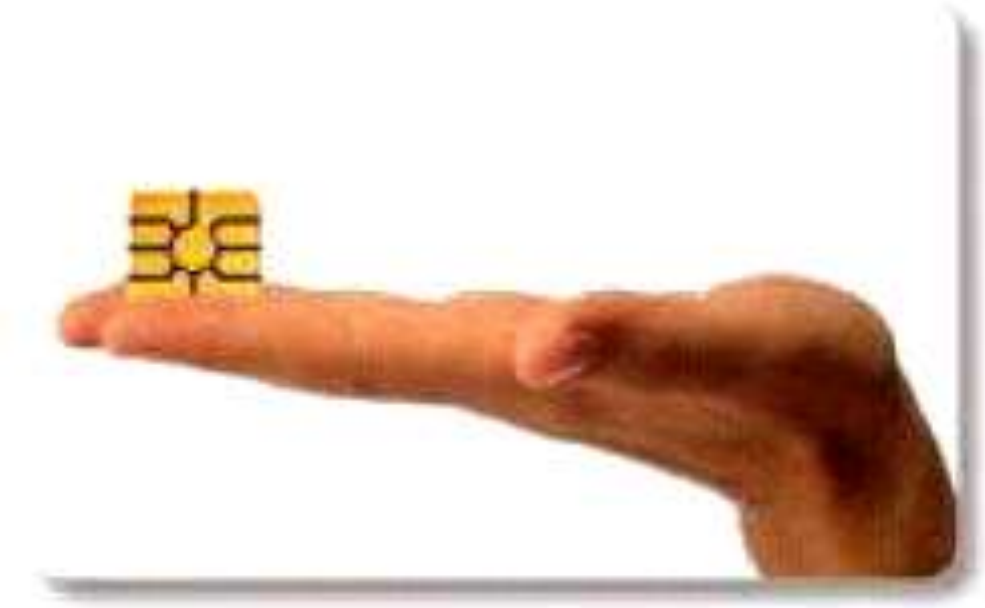
- Svaka individua posjeduje par ključeva.
- Javni ključ svake individue je ovjeren od strane CA (Certifying Authority).
- Javni ključ od CA-a je ovjeren od strane nadzornika (kontrolera).
- Nadzornik sam ovjerava svoj javni ključ.
- Javni ključ svake individue je poznat svim zaiteresovanim i raspoloživ je na Web-u.
- Izvještaj o procesu ovjeravanja je objavljen na Web-u.

UPOREDNI PREGLED KARAKTERISTIKA

Pregled karakteristika različitih vrsta kartica (izvor Most Inc.)			
	Uobičajene magnetske kartice	**Memorijske kartice**	**Pametne kartice**
Broj kartica u upotrebi	> 4 milijarde	oko 330 miliona	oko 100 miliona
Broj čitača u upotrebi	> 5 miliona	?	?
Cena po kartici	$0.05 - 0.5	$0.70 - 1.40	$2.50 - 15
Cena čitača	$100-800	zavisi od područja primene	$100-800
Pouzdanost	mala	srednja	velika
Sigurnost podataka	nikakva	niska	vrlo velika

PRIMJENE "PAMETNIH" KARTICA

Najveća snaga *Smart Card* tehnologije jeste u raznovrsnoj mogućnosti primjene.



PRIMJENE "PAMETNIH" KARTICA

Raznovrsne mogućnosti primjene:

Registracija radnog vremena

Kontrola prolaska

Fizičke blokade

Novčane transakcije

Kantina / knjižara

Sistemi elektronskih brava i cilindara

123456

Automati za hranu

Pristup lokalnoj mreži
Pristup računaru i aplikacijama

Benzinske pumpe

Pranje automobila

FINANSIJSKE "PAMETNE" KARTICE

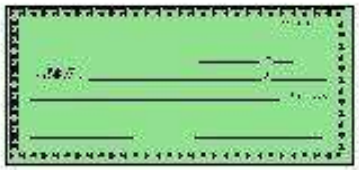
KREDITNA KARTICA
(*CREDIT CARD*)

=

Tek nakon određenog vremena banka naplaćuje dug od korisnika kartice

ČEKOVNA KARTICA
(*DEBIT CARD*)

=



Plaćeni se iznos odmah skida sa pripadnog računa u banci

ELEKTRONIČKI NOVČANIK
(*STORED-VALUE CARDS*)

=

Na kartici je pohranjen "elektronički novac" koji se direktno može koristiti za plaćanje usluga

ZDRAVSTVENA "PAMETNA" KARTICA

- Ljekar može pregledati i modifikovati podatke kartice.
- Preko ličnog računara moguće je pregledati podatke.
- Velika količina podataka, sigurno pohranjena i brzo pretarživanje.
- Izbegava se upotreba velike količine papira.
- Eventualno oštećeni ili izgubljeni podaci se lako nadoknađuju kopijama na računarima.

Zdravstvena kartica u francuskoj

"PAMETNA" KARTICA KAO LIČNA KARTA

“Pametna“ lična karta (eID card) opisuje vlasnika.

Veličine bankovne kartice.

Na kartici su ispisani podaci kao:

- fotografija, ime i prezime, pol, ručni potpis, nacionalnost, mjesto i datum rođenja, Broj lične karte i matični broj.

U čipu se nalaze identifikacioni (biometrijski) podaci i digitalni potpis.

Kartica sadrži brojne zaštite:

- Reljefna stampa, tanke linije, promjenjiva laserska slika, optički promjenjivo mastilo, lasersku štampu, mikro slova, ...

"PAMETNA" KARTICA KAO LIČNA KARTA

Primjene:

- dobijanje zvaničnih dokumenata (izvod iz matične knjige rođenih, materijalni status, ...);
- elektronsko glasanje;
- elektronsko slanje sudskih rješenja;
- autentifikaciju za web sevise (Siguran Chat);
- kontrolu pristupa objektima (magacini, biblioteke, ...);
- online otvaranje novog bankovnog računa;
- siguran potpis;
- online zahtjev za kredit;
- registracija auta;
- autentifikovana pošta;
- elektronsko prikupljanje podataka;
- ...

"PAMETNA" KARTICA I ELEKTRONSKI PASOŠ

Elektronski pasoš je rješenje koje kombinuje tahnologiju pametnih kartica sa biometrijskom tehnologijom.

Bezkontaktni čip je ugrađen u putni dokument (npr. pasoš).

Biometrijski podaci vlasnika pasoša porede se sa podacima na čipu.

"PAMETNA" KARTICA I ELEKTRONSKI PASOŠ

Poreba za sigurnost granice je uslovljena sljedećim ključnim faktorima:

- porast kriminala u svijetu,
- ilegalni prelasci granica, korištenjem lažnih ID dokumenata,
- povećanje efikasnosti i ekonomičnosti u upravljanju velikom količinom podataka o osobama.

Nova generacija ID i putnih dokumenata sadrži pametne čipove i biometrijske podatke vlasnika. Gotovo ih je nemoguće falsifikovati.