Univerza v Ljubljani

Fakulteta
za računalništvo
in informatiko

Varnost, zaščita in kriptiranje

Mojca Ciglarič

UVOD (1/3)

- Varnost - kaj je, kdo je ogrožen, kaj ga ogroža?
- Varovanje: preprečevanje možnih nevarnosti
- Ranljivost: šibka točka sistema
- Organizacijski del je danes **pomembnejši** od tehnološkega!
- Dve področji varnosti:
  - **Zanesljivost**: zagotavljanje razmer za delovanje storitev in normalno delo uporabnikov
  - **Zaščita**: onemogočanje nelegalne uporabe sistema
- Oboje lokalno ali razpršeno, zanima nas bolj razpršeno.
- Nadzor!
- Vloge: nadzornik/upravljalec, vzdrževalec, napadalec, uporabnik

Zagotavljanje zanesljivosti (2/3)

- **Ustrezen nadzor**: zbiranje podatkov o delovanju, stanju, uporabi sistema. Dnevniki.
- **Upravljanje**: ukrepanje na podlagi zbranih podatkov.
- Alarmi.Diagnostika. Načrtovanje. Administracija.
- **Orodja**: imeniki, seznami in kazala. SNMP. Poslovna pravila.
- Načrtovanje zmogljivosti in razvoja sistema, primerno testiranje in uvajanje.
- **Razpršena zaščita**. Integriteta povezav, virov, vsebine, uporabnikov, sporočil.

Zaščita in kriptiranje (3/3)

- Kriptiranje: skrivanje vsebine
- Zgodovinski kriptografski postopki

- Simetrični algortimi (DES, AES)
- Asimetrični algoritmi (RSA, ECC)

- Kriptoanaliza (razbijanje)

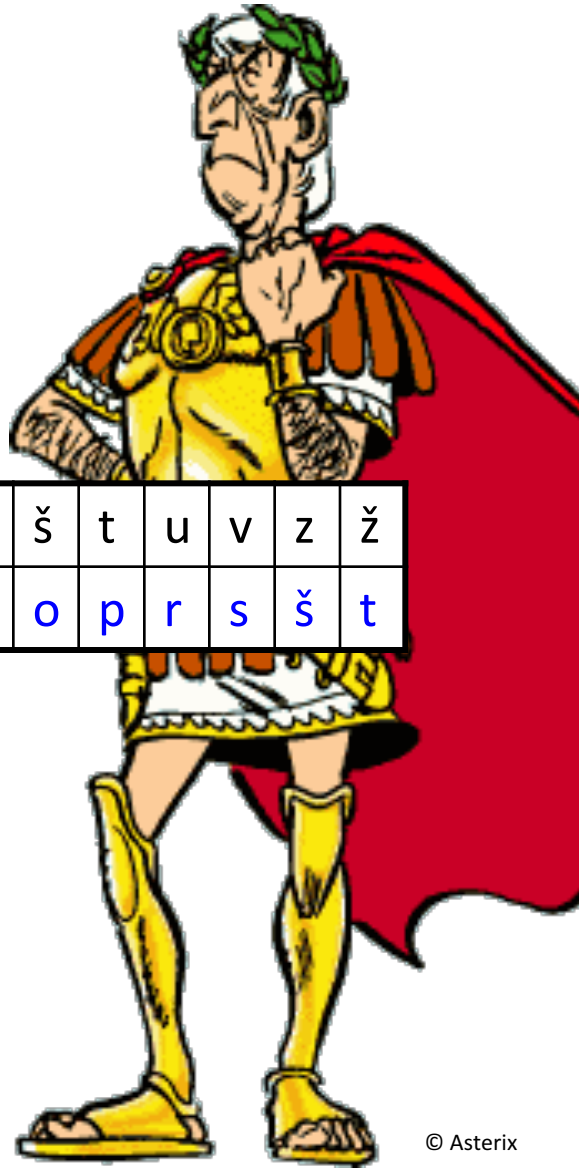
Kriptografske metode

- Po načinu
  - Substitucijske: posamezne črke ali dele besedila nadomestimo z drugimi.
  - Transpozicijske: spreminjamo vrstni red znakov, besed, stavkov…
- Po lastnostih ključa
  - Simetrične: E=D, ključ mora biti tajen.
  - Asimetrične: E≠D, E je lahko javen, D mora biti tajen.

Klasične metode: Cezar

- Cezarjev kriptogram: substitucija.
- JULUA = ?

a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž
u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t



© Asterix

- 25 možnih ključev
- Razbijemo ga v največ 25 poskusih!

Razbijanje substitucijskega kriptograma

- Razbijanje na osnovi poznanega besedila (npr. “please login”) – že v 1. poskusu!
  - Zato kriptiramo le vsebino, ne cele komunikacije
- Statistika jezika (črke, besede, dvo- ali tročrkovni sklopi) – potrebno je daljše besedilo.
- Poznavanje vsebine (semantika) olajša razbijanje – iščemo pričakovane korene besed ipd.

Vigenèr-jev kriptogram – večabecedno kriptiranje

- Preprost ključ
- Statistika jezika in semantika postaneta nemočni
- Viegenerjeva matrika: vse Cezarjeve abecede.

a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž
b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a
c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b
č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c
d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č

(in tako dalje še 20 vrstic…)

- Ključ = niz D črk, vsaki pripada ena vrstica (enaka 1. črka).
- Z abecedo n-te črke gesla kriptiramo n-to, n+D-to, n+2D-to … črko sporočila.

Vigenèr-jev kriptogram (primer)

- Ključ: računalniške komunikacije
- Sporočilo: Junija vsi izpiti na žalost odpadejo, razen pri ekonomiki, septembra pa bo spet vse po starem.

r	a	č	u	n	a	l	n	i	š	k	e	k	o	m	u	n	i	k	a	c	i	j	e
j	u	n	i	j	a	v	s	i	i	z	p	i	t	i	n	a	ž	a	l	o	s	t	o
d	p	a	d	e	j	o	r	a	z	e	n	p	r	i	e	k	o	n	o	m	i	k	i
S	e	p	t	e	m	b	r	a	p	a	b	o	s	p	e	t	v	s	e	p	o	s	t
a	r	e	m																				

- Prvi stolpec črk kriptiramo z 18. abecedo, itd.

Porterjev kriptogram

- Kriptiramo po 2 znaka hkrati.
- Simboli so v tabeli – vrstica za en, stolpec za drugi znak.

	a	b	c	č	d	e	f	g	h	i	j	k	l	m
a														
b														
c														
č											…	it	d	…
d														

- npr. KAČA = 

Kodiranje

- Cel znak ali besedo nadomestimo z drugo.
- Ni splošnega pravila za zamenjave.
- Ključ predstavlja cela kodna tabela.

"Bugger! I was just about to crack his code, when he burnt his blanket."

Transpozicijski kriptogram

- Znake ali dele besedila premestimo!
- Ključ ima vse črke različne (npr. KOPRIVA).
- Oštevilčimo ključ po abecedi.
- Zapišemo stolpce glede na številke.

k	o	p	r	i	v	a
3	4	5	6	2	7	1
J	u	n	i	j	a	n
ž	a	l	o	s	t	v
s	i	i	z	p	i	t
i	o	d	p	a	d	e
j	o	b	l	a	b	l

Klasične metode - povzetek

- Klasične metode – zgolj za razumevanje.
- Znakovno usmerjene – kriptiramo črko po črko (včasih tudi po besedah).
- Z računalniki jih ni težko razbijati.
- Sodobne računalniške metode so bitno usmerjene.

Simetrične kriptografske metode

- DES
- AES
- IDEA
- RC4
- Misty

Osnovni elementi simetričnih metod

- Transpozicija (P-škatla, ključ)
  - Permutacija
  - Redukcija
  - Ekspanzija
- Substitucija (S-škatla, tabele)
  - Dekoder $n/2^n$ (poljuben n-bitni vhod $\longrightarrow$ same 0 in 1 enica – po tabeli)
  - Permutacija
  - Koder $2^n/n$ (obratno kot dekoder – po tabeli)

DES

- Simetričen.
- Hiter (strojna implementacija).
- Kaskada zaporednih permutacij, substitucij in še nekaterih operacij.
- Deluje nad 64-bitnimi binarnimi bloki.
- Ključ je 56-biten.
- Težave z distribucijo ključa!
- Sum bližnjice…
- Več – podrobno: na vajah!

Metoda enkratnega ključa

- Ključ je daljši kot besedilo.
- Ekskluzivni ALI (xor): (A xor B) xor B = A
- Enkripcija: P xor E = E(P)
- Dekripcija: D(E(P)) = E(P) xor E
  = (P xor E) xor E = P
- Težava: potrebno je generirati poljubno dolg ključ (na obeh straneh! - sinhronizacija)

Veriženje

- DES ali AES = velik substitucijski kriptogram!

M	O	J	C	A		e	u	r		1	0	0	0	.	0
J	A	N	E	Z		e	u	r		3	0	0	0	.	0
P	E	T	E	R		e	u	r			6	2	0	.	0

- Možno je zamenjati posamezne kriptirane bloke z drugimi, tudi če ne poznamo ključa.

Enkripcijski stroj (veriženje)

Metoda enkratnega ključa ima težave s ključi.

- Kompromis: Naslednji blok sporočila najprej XOR-kriptiramo s prejšnjim kriptiranim blokom, šele nato ga zares kriptiramo.
- $C_N=E(P_N \text{ XOR } C_{N-1})$

Načini uporabe bločnih kriptosistemov

- CBC (Cypher Block Chaining) – osnovno veriženje:
  - Pred kriptiranjem se vsak blok XOR-a s prejšnjim kriptiranim blokom.
- PCBC (Propagating CBC) – upošteva več prejšnjih P in C blokov
- CFB (cipher Feedback) – zelo podobno.Omogoča tudi kode za popravljanje napak (napačen bit na istoležnem mestu).
- CTR (counter) – za vzporedno kriptiranje več blokov hkrati.

- Potreben je inicializacijski vektor: težave z distribucijo!

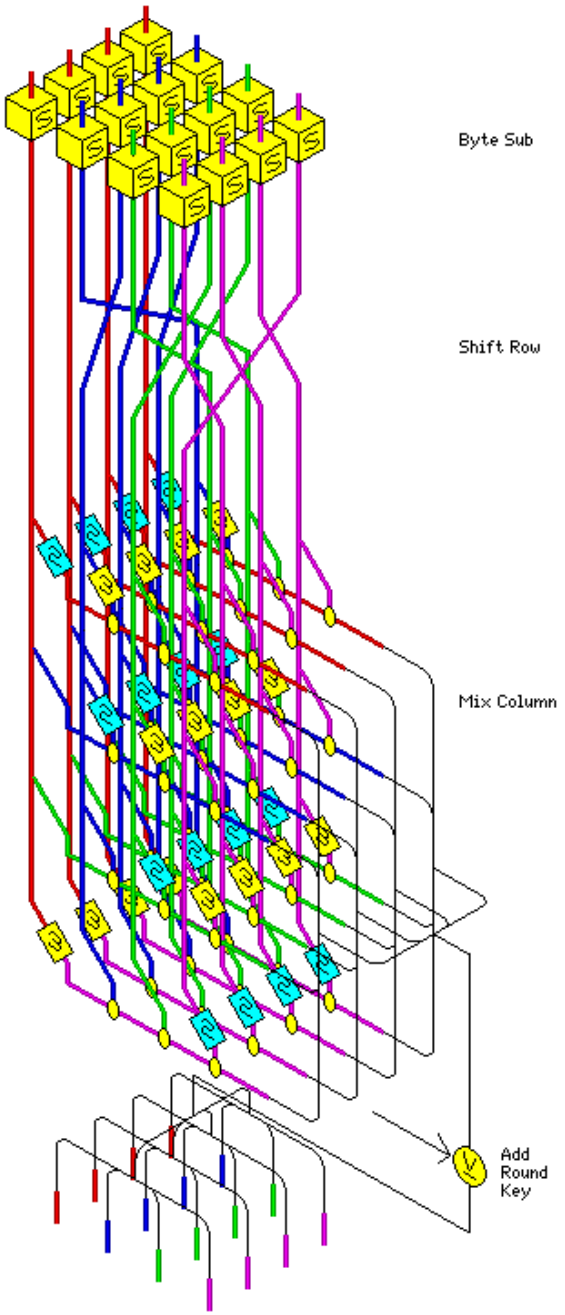
Trojni DES

- 3 x kriptiranje
- 3 x počasnejši
- 2^{56} x varnejši za napad z grobo silo

- Enkripcija: E(K1) – D(K2) – E(K1)
- Dekripcija: D(K1) – E(K2) – D(K1)
- 112 bitov je dovolj varno.
- EDE namesto EEE: za kompatibilnost med DES in 3-DES (3-DES rač. nastavi K2 = K1)

AES: simetričen

- Advanced Encryption Standard
- Rijndael: kriptografski algoritem (Daemen, Rijmen)
- Hiter, varen
- Blok dolg 256 (16 8-bitnih znakov)
- Ključ dolg različno (128, 196, 256)
- Dekripcija: v obratni smeri ali z drugimi tabelami.



AES: osnovne operacije

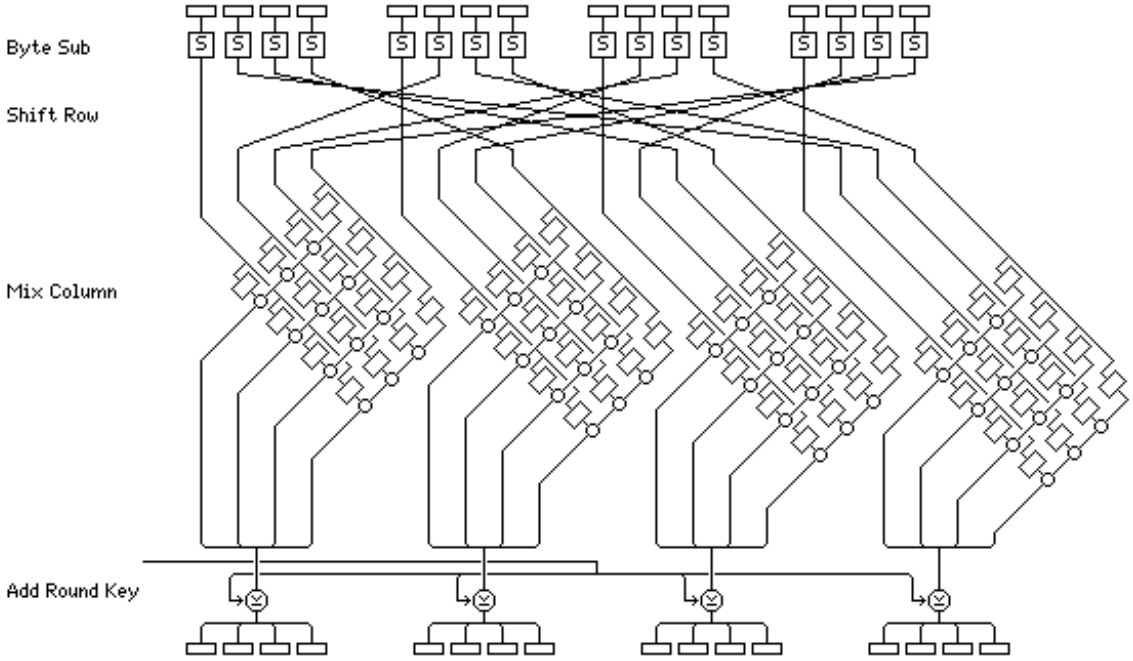
- Byte sub: Substitucija (S-škatla)
- Shift row: mešanje vrstic (P-škatla)
- Mix column: mešanje stolpcev – substitucija, ki temelji na aritmetiki končnih polj.
- Add round key – substitucija:
  XOR trenutnega bloka z delom ekspandiranega ključa.

- Vizualizacija:
  https://www.youtube.com/watch?v=mlzxpkdXP58

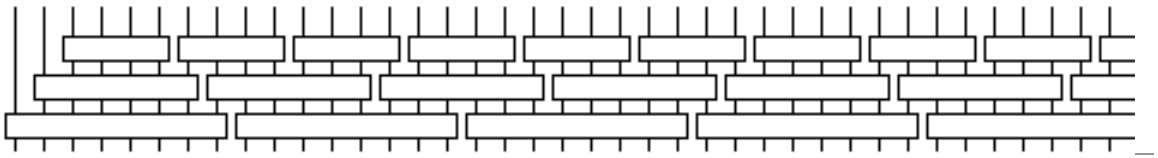
AES: simetričen

http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

Shema z drugega zornega kota:



Možno sestavljati različne dolžine ključev kot lego kocke:



Drugi simetrični algoritmi

- IDEA, 1990 (International Data Encription Algorithm)
  - Podoben DES-u, brez večjih slabosti
  - Uporaba v PGP (+ triple DES +CAST)
- RC2 (Rivest Cipher 2)
  - Eden od algoritmov S/MIME
  - Spremenljiva dolžina ključa
- CAST (imena avtorjev) –(v PGP)
  - RFC2144: določene S-škatle in 128-bitni ključ
  - RFC2612: CAST-256 s spremenljivo dolžino ključa
- Skipjack, Misty
- ...

Asimetrična kriptografija

- E in D različna!
- E je lahko javen, D mora biti tajen.
  - D(E(P)) = P
  - Iz P in E(P) je nemogoče ugotoviti D.
  - Iz E je nemogoče ugotoviti D.

RSA

- Izberemo p,q: veliki praštevili (1024 bitov)

$$n = pq$$

$$z = (p-1)(q-1)$$

- Izberemo d: nima skupnih deliteljev z *z*.
- Izberemo e: *ed* mod *z* = 1
- P $\rightarrow$ $C=P^e$ mod *n* *kriptiranje*
- C $\rightarrow$ $P=C^d$ mod *n* *dekriptiranje*
- *Ni težav z distribucijo. Počasnost.*

Elektronski podpis

- To je medsebojno identificiranje uporabnikov.
- Potreben pogoj: D(E(P) = E(D(P))
- Oddajnik sporočilu doda informacijo, ki je značilna samo zanj.
- Za podpis se navadno uporabi le kratek niz P (nekaj 100 bitov): lahko digitalni izvleček.
  - Ime in priimek
  - EMŠO, davčna, vpisna številka, …
  - Podjetje
  - Datum in ura podpisa

Elektronski podpis z RSA

- Pogoj: E(D(P))=D(E(P))
- Podpis: informacija, lastna samo podpisniku: D; D(P) je podpisano besedilo.
- Peter: E_P, D_P
- Vesna: E_V, D_V

- P="Peter Klepec" $\rightarrow$ podpisano:$D_P(P)$
- Enkripcija: $E_V(D_P(P)) \rightarrow$ sledi prenos.
- Dekripcija: $D_V\,(E_V(D_P(P)) = D_P(P)$
- Preverjanje podpisa: $E_P(D_P(P)) = P$

Tajenje podpisa

- Če podpisnik zamenja ključ, lahko taji svoje prejšnje podpise!
- NOTAR ali OVERITELJ: uporabnik deponira svoje podatke skupaj s časom njihove veljavnosti
- Notar vzdržuje tudi historiat.
- Notarju zaupamo!
- Ko prejmemo podpisano sporočilo, preverimo podpis pri notarju.

Zgoščevalne funkcije – digitalni izvlečki:

- Izvleček (hash) sporočila *m: f = h(m)*
- *m* je poljubno dolgo sporočilo
- *f* je kratek (omejene dolžine!).
- Kolizija: različna sporočila imajo enak izvleček.

Dobra zg. funkcija

- Pri vseh možnih vhodnih vrednostih je frekvenca vseh rezultatov enaka.
- Majhna sprememba sporočila povzroči veliko spremembo podpisa.
- Zelo težko najti drugačno vhodno vrednost za isti podpis (kolizijo)!
- Take funkcije imenujemo *cryptographic hash value, digital fingerprint, footprint, message digest (MD), cryptographic checksum*.

Način delovanja zg. funkcij

- Preproste bitne operacije brez ključa
- Podobno simetrični kriptografiji
- Delitev sporočila v bloke
- Procesiranje blokov v več ciklih
- SHA-1 (trenutno najpomembnejši!) – 160 bitov
- MD4 (podlaga za SHA-1) in MD5 – 128 bitov
- Zgoščevalna funkcija s ključem: MAC (Message Authenticy Check)

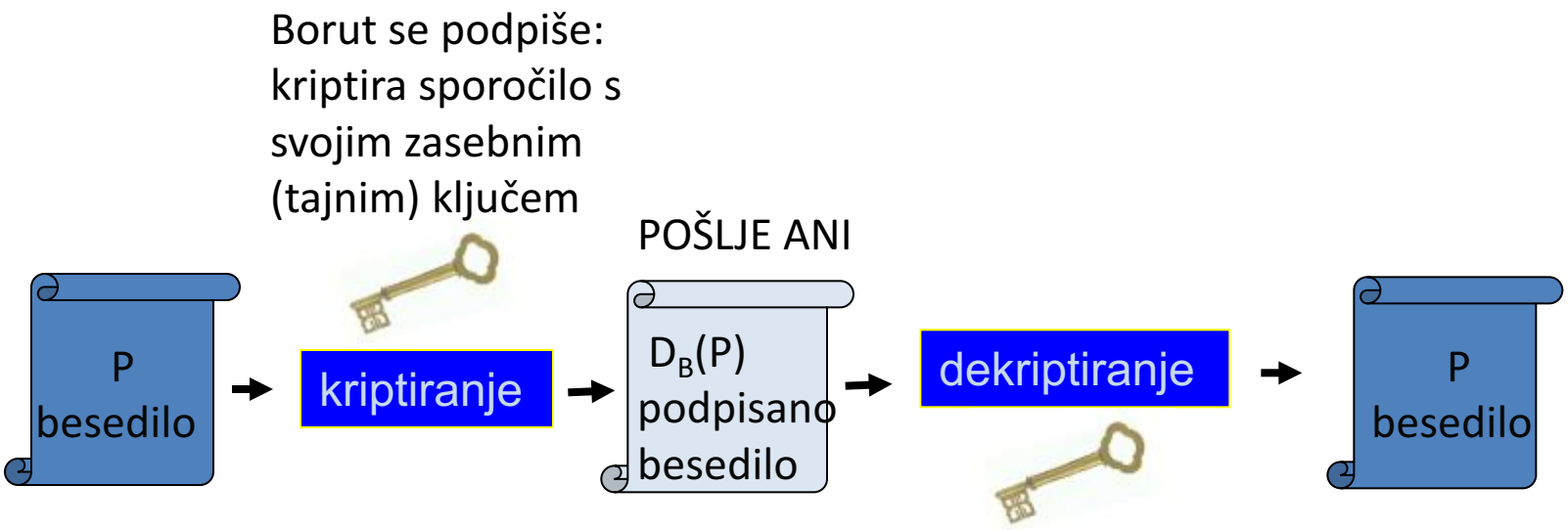
Integriteta sporočila

- Ali je bilo sporočilo med prenosom spremenjeno?
- Digitalni izvleček sporočila Z(P)
- Z(P) podpišemo in pošljemo skupaj s sporočilom.

Zagotavljanje integritete sporočila

- Kako vem, da ni bilo sporočilo med prenosom spremenjeno?
- Zagotavljanje integritete pomeni mehanizem, s katerim ob prejemu lahko ugotovimo, ali je bilo sporočilo med prenosom spremenjeno.

Podpis podatkov



Če želimo ohraniti tudi zaupnost sporočila, ga je treba po podpisu še kriptirati z Aninim javnim ključem E_A.
Sam podpis ne zagotavlja zaupnosti, saj je E_B javni ključ, ki ga lahko dobi kdorkoli!

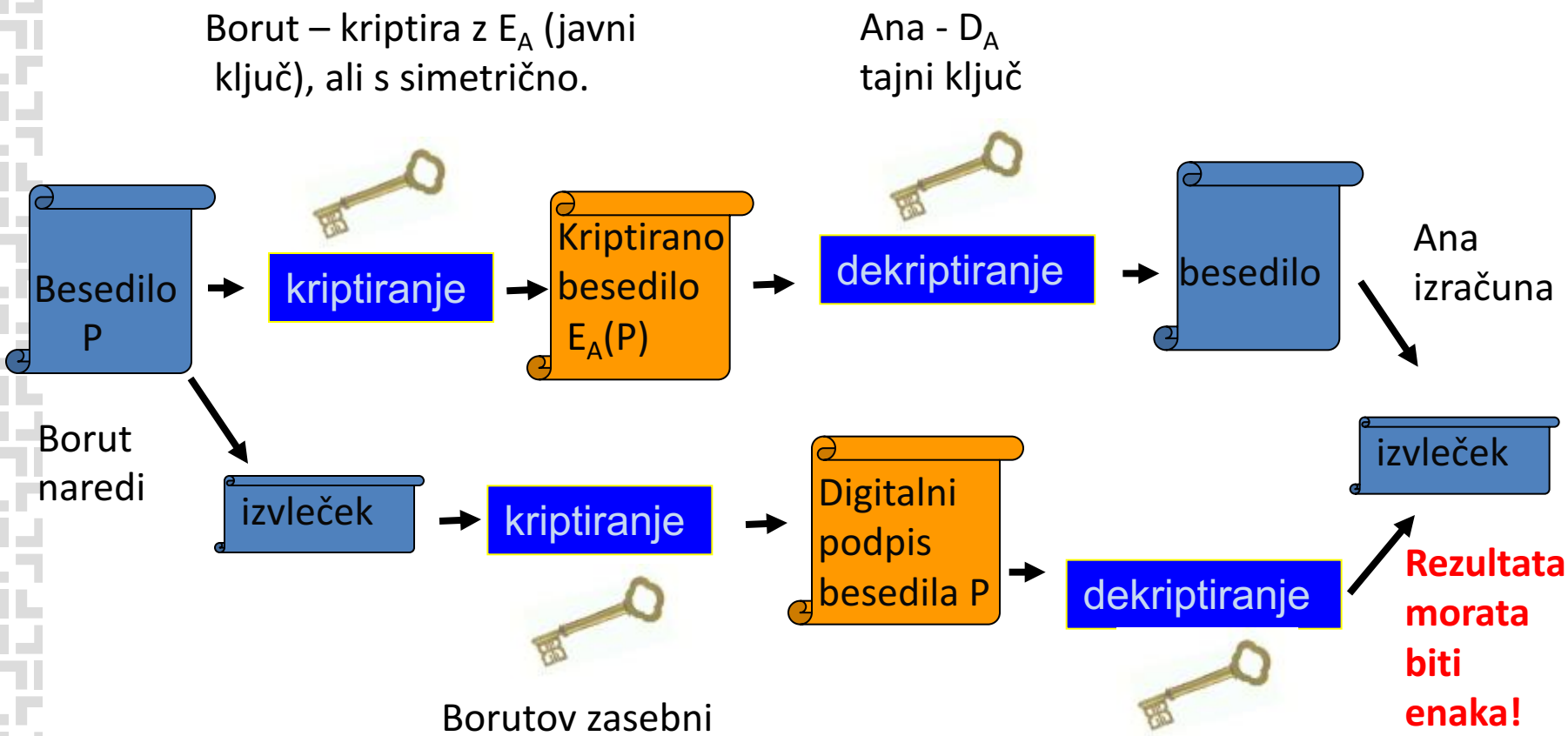
Ana: preveri podpis
- dekriptira z Borutovim javnim ključem: $E_B(D_B(P))$

Integriteta sporočila

- Podpisovanje celotnega sporočila je zamudno.
- Včasih zaupnost ni potrebna.
- Lahko podpišemo le izvleček.

1. Sporočilo
2. Naredimo izvleček
3. Podpis izvlečka (tajni ključ pošiljatelja)
4. (Kriptiranje) – če je potrebno (javni ključ prejemnika ali simetrični sejni ključ)

Zagotavljanje identičnosti sporočila (izvleček)



Generatorji

- Naključni generatorji, vgrajeni v OS, prevajalnik, … : statistično dobro porazdeljeni
- Generator naključnih števil
  - Čas med dostopi do diska
  - Vnosi s tipkovnice
  - Premiki miške
  - Strojni: spremembe napetosti
- Generator praštevil
  - Temelji na zgornjem
  - Preverja delitelje

Varna komunikacija

- Zaupnost – kdo sme prebrati? (enkripcija)
- Avtentikacija – dokaži, da si res ti,
- (Identifikacija – povej, kdo si - brez dokaza)
- Integriteta sporočila – je bilo med prenosom spremenjeno?
- Preprečevanje zanikanja (nonrepudiation) – res si poslal / res si prejel.
- Razpoložljivost in nadzor dostopa – preprečevanje nelegitimne rabe virov (avtorizacija – ugotavljanje, ali nekaj smeš storiti)

- Pomembno je tudi beleženje vseh dogodkov (dostopov, ...)

Problemi

- Poznamo kriptografske metode
  - simetrične,
  - asimetrične.
- Kako ugotoviti, s kom ZARES komuniciram? AVTENTIKACIJA
- Kako se prepričati, da sporočilo med prenosom ni bilo spremenjeno? INTEGRITETA
- Kako distribuirati javne ključe?

Avtentikacija

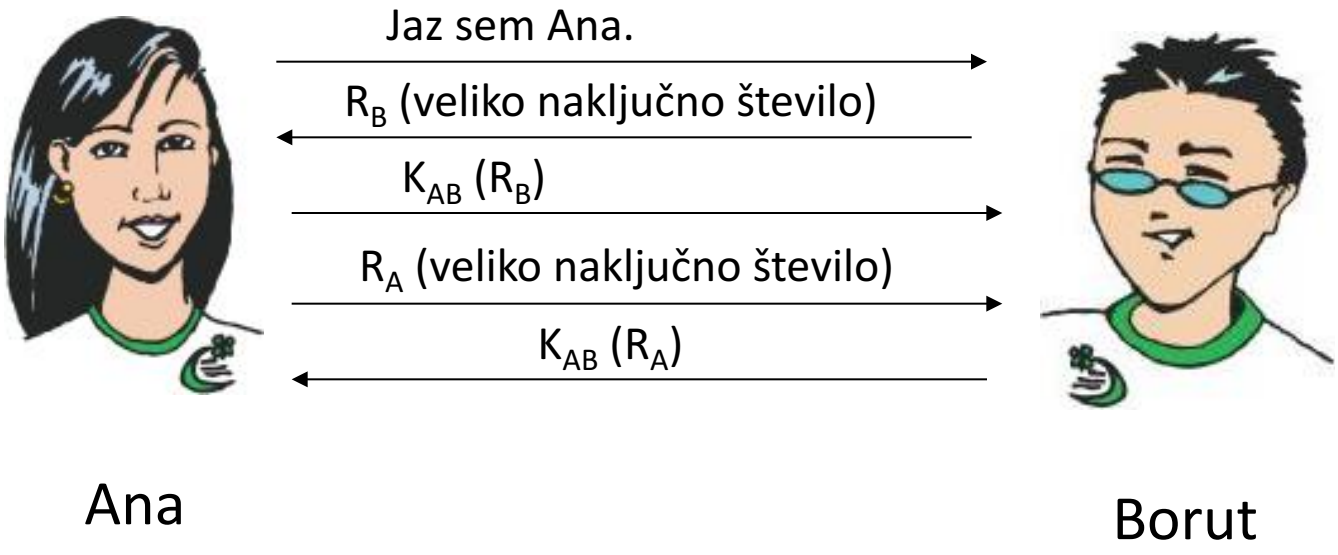
- Če vem, kdo si, ti dovolim več:
  - Se pogovarjam s tabo
  - Dostop do podatkov (avtorizacija)
  - Ti zaupam (verjamem)
- Osebna izkaznica, geslo, kreditna kartica
- To omogoča tudi PKI (infrastruktura javnega ključa) .

Avtentikacija

- Prepričamo se, da je naš sogovornik res tisti, za kogar se izdaja. Tri principi:
  - Izziv-odgovor (vnaprej se dogovorimo za skupno skrivnost)
  - Zaupamo tretji strani
  - Avtentikacija z javnim ključem

Protokol izziv-odgovor

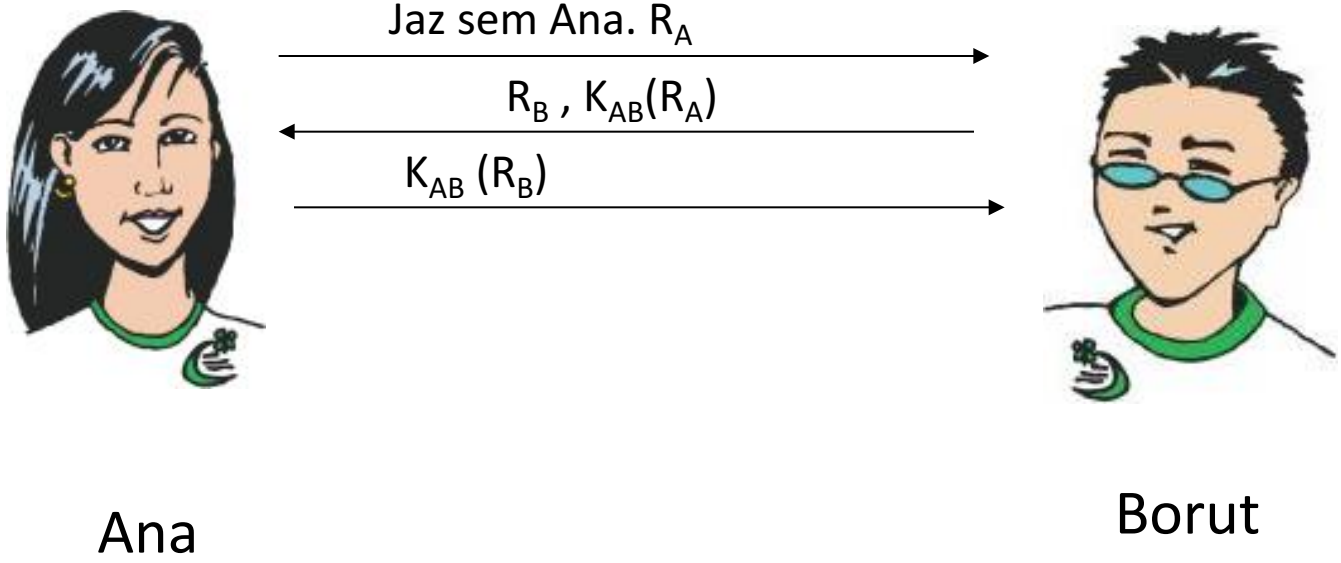
- *Challenge-Response* ali *Shared Secret*
  - Dvosmerna avtentikacija. K_{AB} je vnaprej znan.
- Primer:



Protokol izziv-odgovor

Malo skrajšan primer:

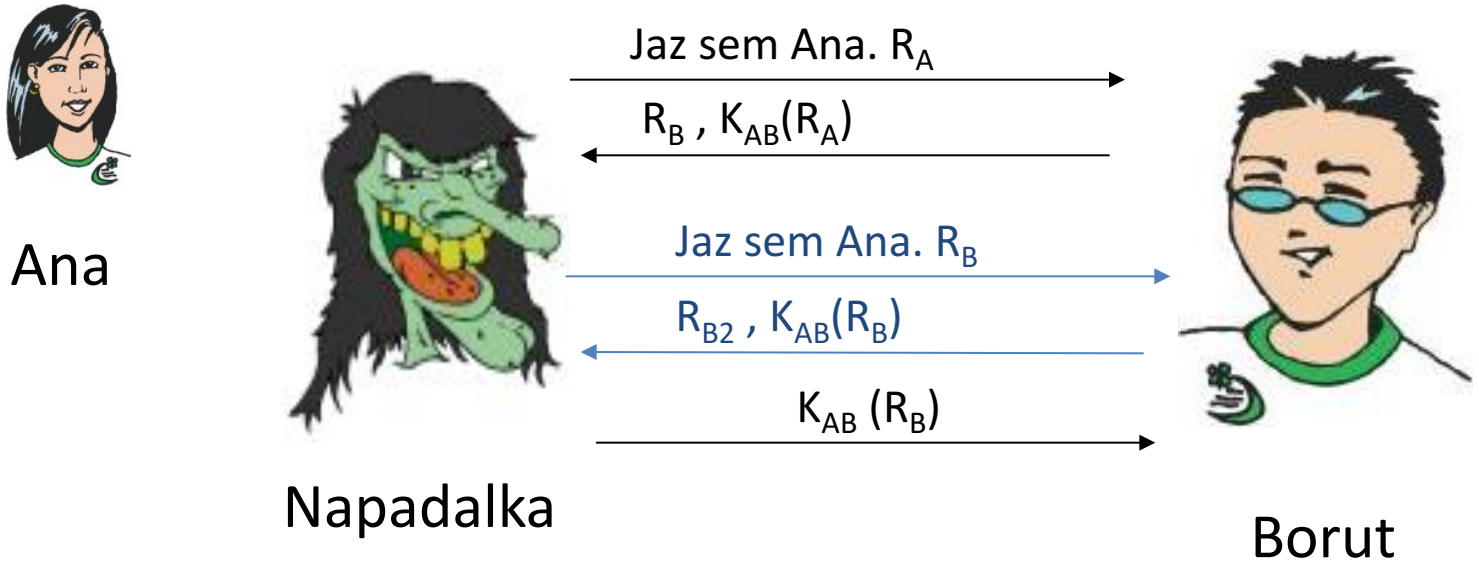
- Je varen?



Protokol izziv-odgovor

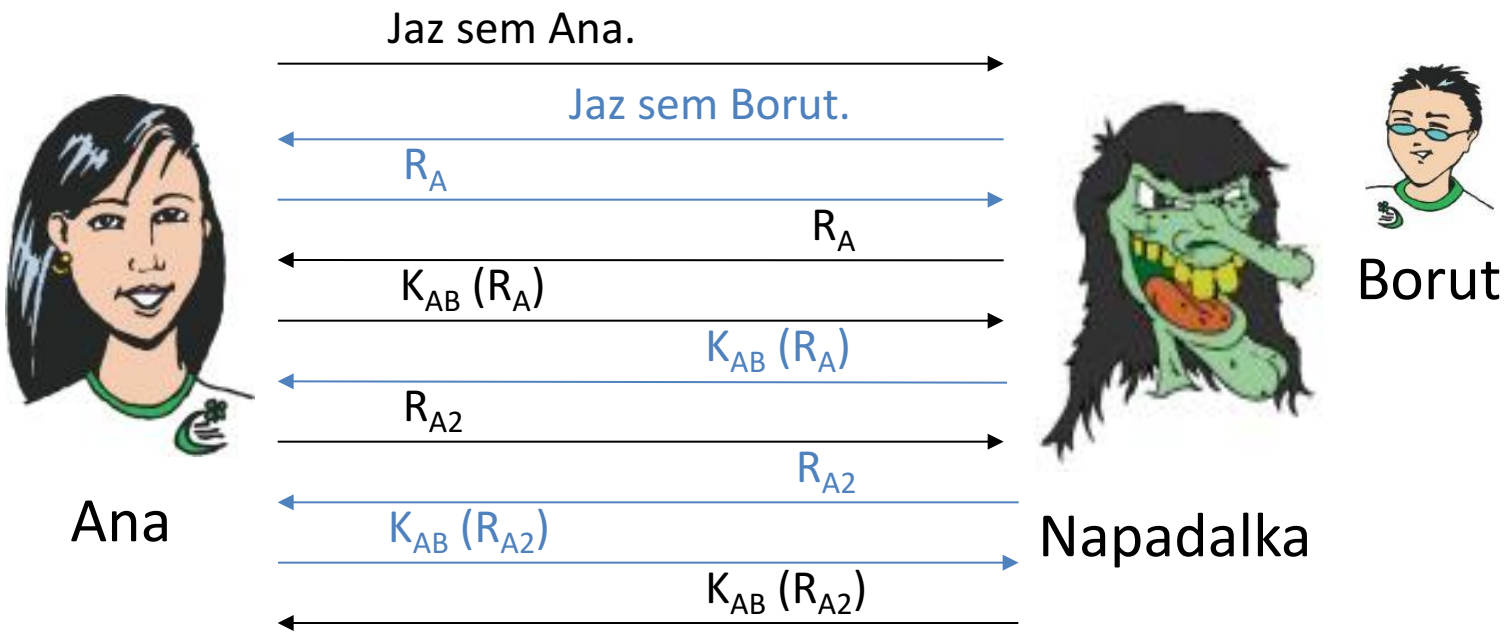
Malo skrajšan primer

- Napad z zrcaljenjem(reflection attack) – če B omogoča več sej hkrati.



Protokol izziv-odgovor

- Napad z zrcaljenjem na prvi protokol:

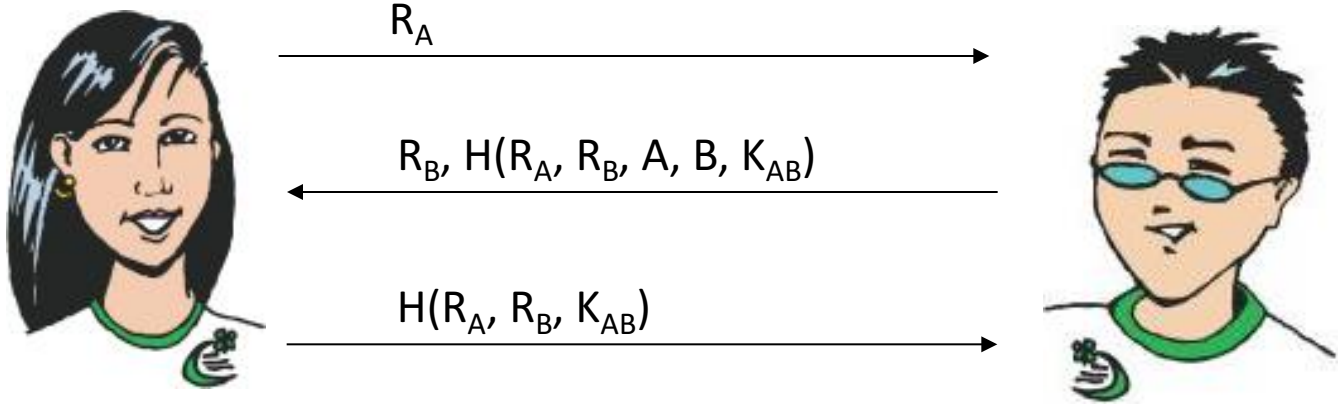


Varen protokol izziv-odgovor

- TEŽKO!
- Pravila:
  - Iniciator naj prvi dokaže svojo identiteto.
  - Za dokaz naj uporabljata različne ključe (K_{AB} in K_{BA})
  - Izziva (R) naj bosta različna (npr. sodo-liho št.)
  - Informacija iz ene seje nekoristna v drugi seji.

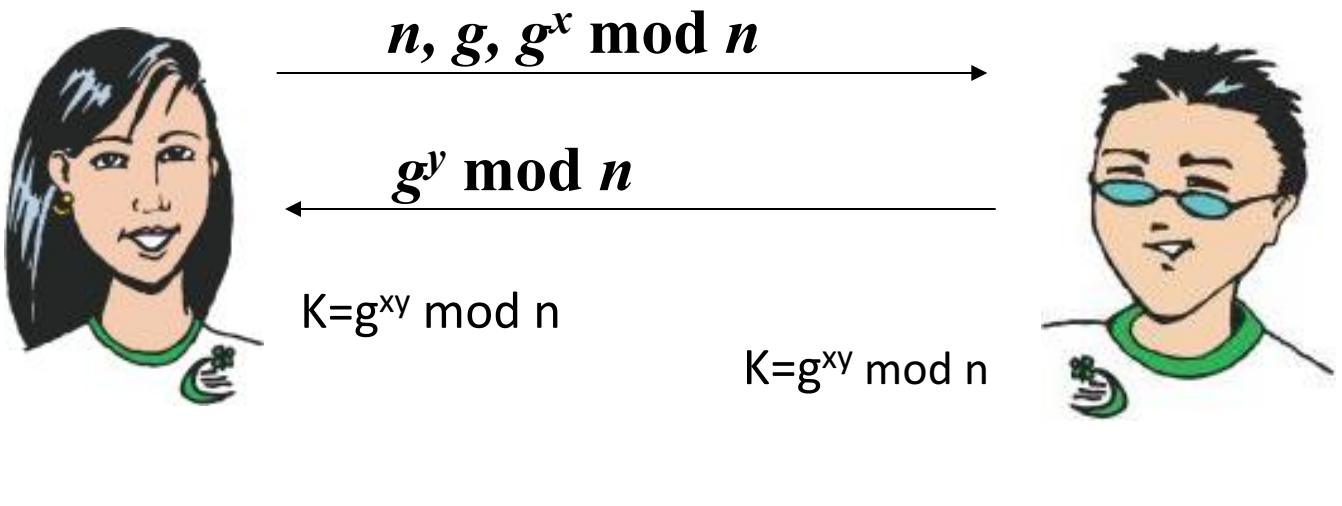
Varen protokol za avtentikacijo

- Uporablja zgoščevalne funkcije (digitalni izvleček)!



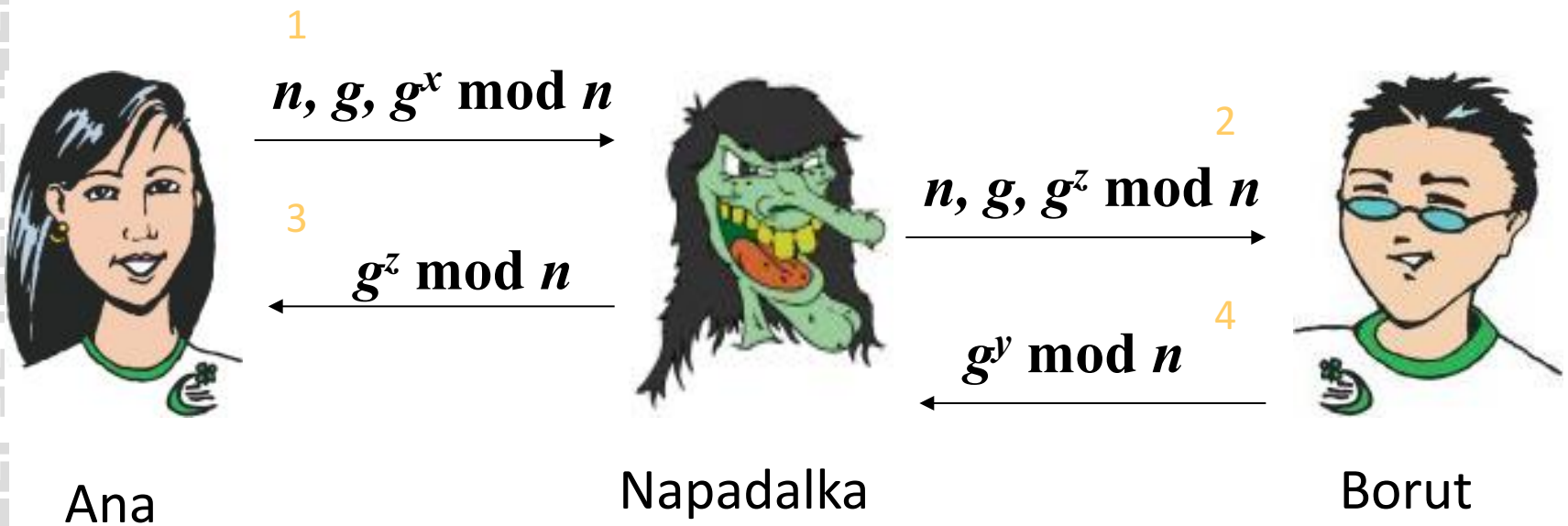
Diffie-Hellman izmenjava ključev

- Kako si pred avtentikacijo izmenjata K_{AB}?
- Najprej izbereta n in g – javno.
- Eden izbere x, drugi y – tajno.



Diffie-Hellman izmenjava ključev

- Napad z vrivanjem (man in the middle attack).

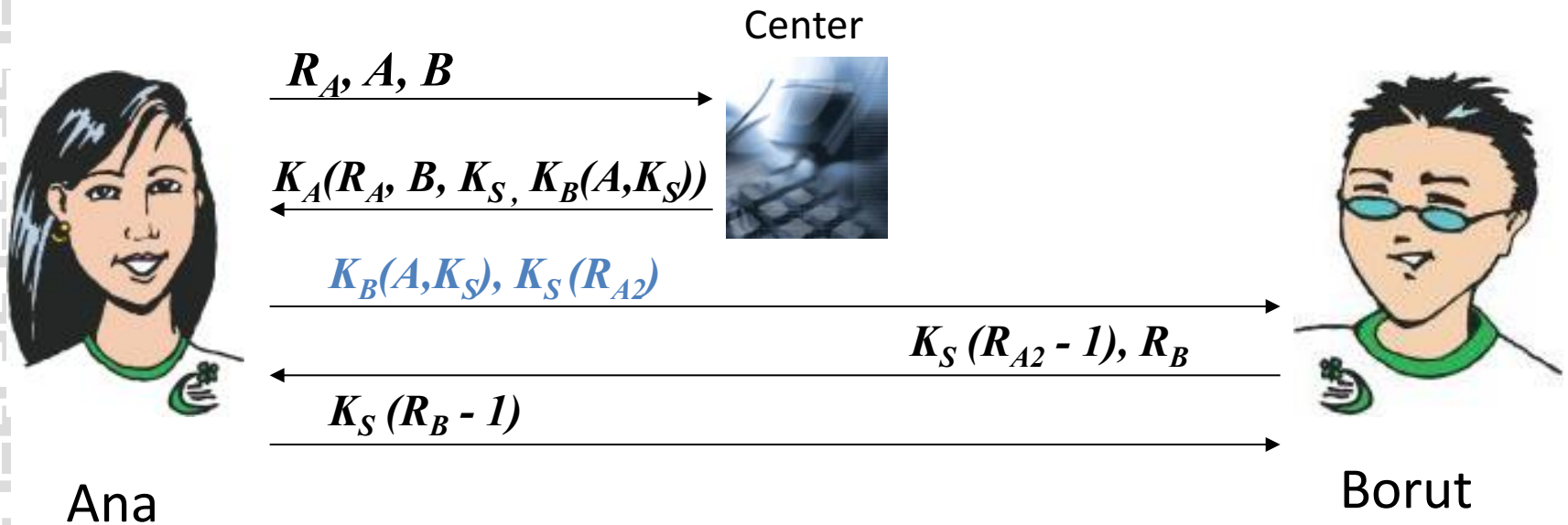


Center za distribucijo ključev

- Težava: upravljanje in organizacija ključev.
- Center pozna vse tajne ključe. Zaupanje!
- Možen napad: replay attack – napad s posneto sejo.
  - Nepooblaščena ponovitev legalne seje (npr. plačilo računa).
  - Rešitev: časovno označevanje in/ali izziv R v vsakem sporočilu

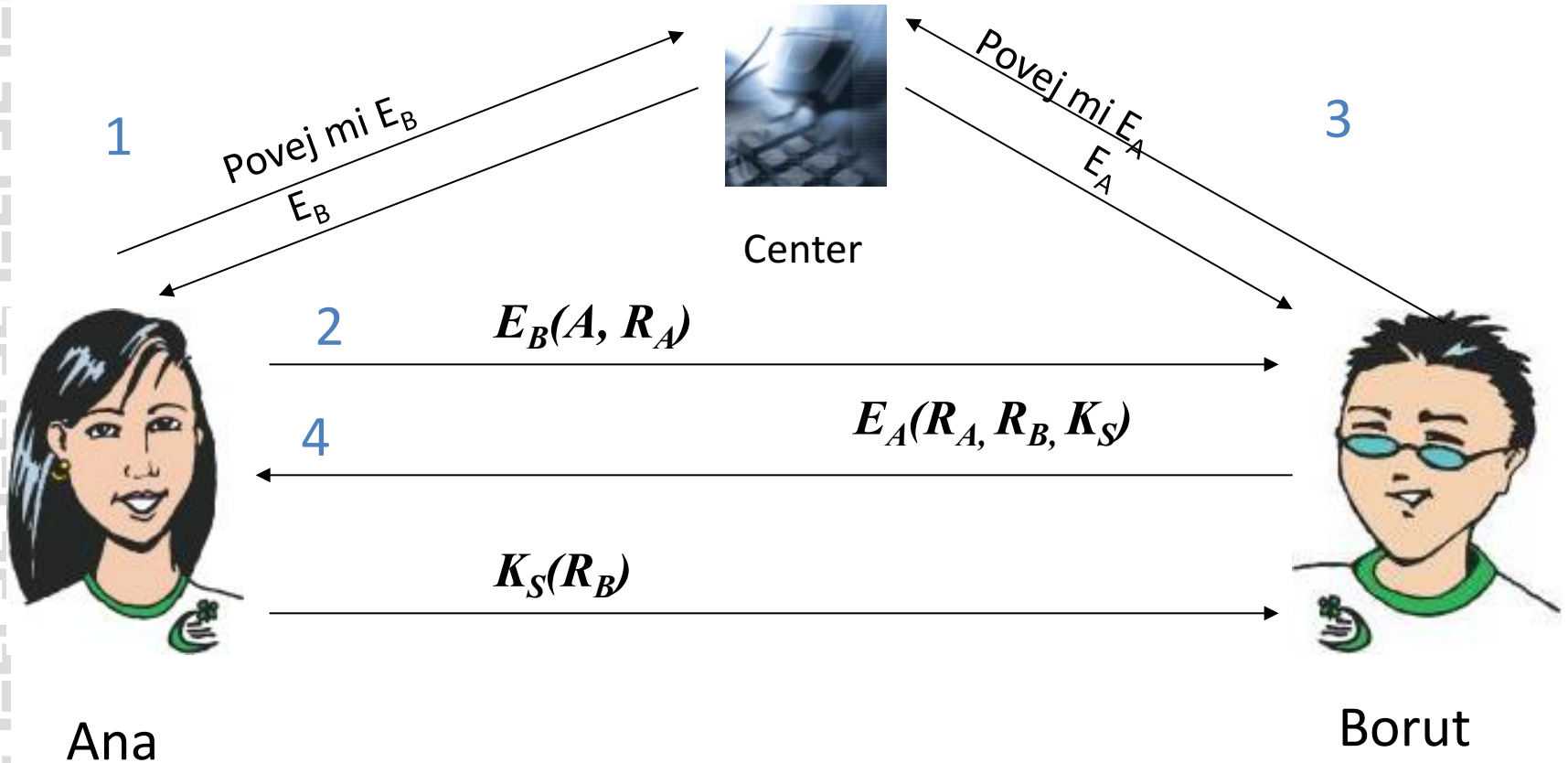
Center za distribucijo ključev

- Needham-Schroeder:
- Če napadalec dobi star K_S, še vedno lahko napade na 3. koraku (replay)!



Avtentikacija v PKI

- Varno, če zaupamo centru.



Kerberos

- Avtentikacija s pomočjo simetričnih ključev + strežnik za hranjenje in distribucijo ključev in nadzor dostopa.
- Avtentikacijski strežnik (AS) = center za distribucijo ključev.

- Odjemalec A želi dostop do strežnika B. A in AS si dogovorita za kriptiranje seje.
- AS preveri , če A sme uporabljati B. Če da, izda A-ju vstopnico (A, B, sejni ključ K_S, veljavnost) in jo kriptira s K_B.
- A pošlje Bju vstopnico in svoj izziv, kriptiran s K_S.
- B dekriptira vstopnico in nato še odgovor na izziv, spet kriptiranega s K_S.

Radius (RFC 2865, 2866 ,...)

- AAA strežnik (avtentikacija, avtorizacija, zaračunavanje)
- Uporabnike lahko preverja v zunanjem imeniku (AD, LDAP, Kerberos...)
- Strežnik zavrne dostop, zahteva izziv, ali pa sprejme zahtevo.
- Uporaba v Wi- Fi omrežjih, pri SIP- ponudnikih itd...
- Nadomestil ga bo protokol Diameter (d = 2r) ?
  - TCP namesto UDP
  - Uporablja varnen kanal (IPSec ali STCP).
  - ....

Naloge CA:

- Preverjanje identitete: ali si ta, za kogar se izdajaš (uporabnik, program, računalnik, usmerjevalnik...).
- Ustvarjanje digitalnega potrdila in povezave z identiteto posameznika (Id potrdila, javni ključ in podatki o lastniku)
- Podatki v digitalnem potrdilu:
  - Verzija specifikacije X.509
  - ID
  - Algoritem za podpis
  - Začetek in konec veljavnosti ključa
  - Podatki o lastniku.

Digitalni certifikat (ali elektronsko potrdilo)

- Zaupanja vredna avtoriteta (certifikatna agencija - CA) - pri nas so kvalificirani **NLB, Pošta, SiGen, Halcom.**
  - **Kvalificiran** overitelj izpolnjuje stroge zakonske pogoje
- CA mora imeti dobro definirana pravila (politiko) izdajanja certifikatov (kdo, kako, pod kakšnimi pogoji ga dobi).
  - Primer: http://postarca.posta.si/files/postarca/politika_fizicne_kartica_v1.pdf
- CA podpiše uporabnikove osebne podatke – “vizitko”: to je digitalno potrdilo ali certifikat, je časovno omejen.
- Tega nato uporabnik uporablja za avtentikacijo. Certifikatu zaupamo, ker je podpisan s strani zaupanja vredne avtoritete.

X.509

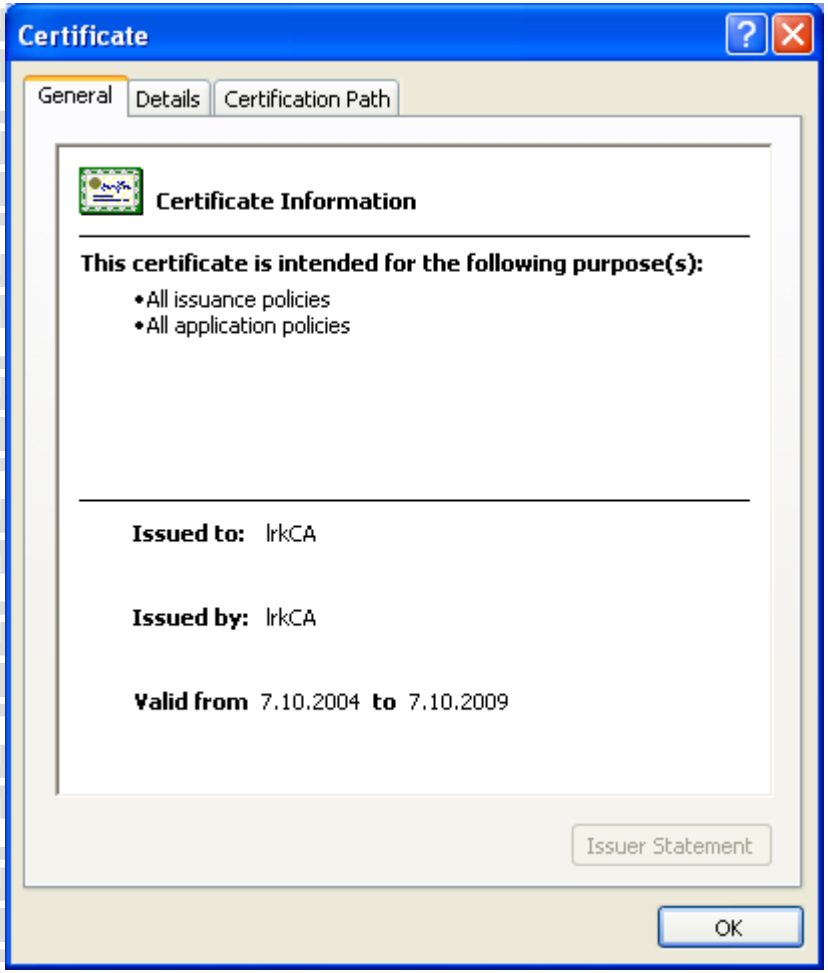
- X.509 v3: ITU-T / IETF PKI standard
  - Format certifikata
  - Postopek preverjanja veljavnosti certifikata
  - CRL
- Zahteva hierarhijo CA

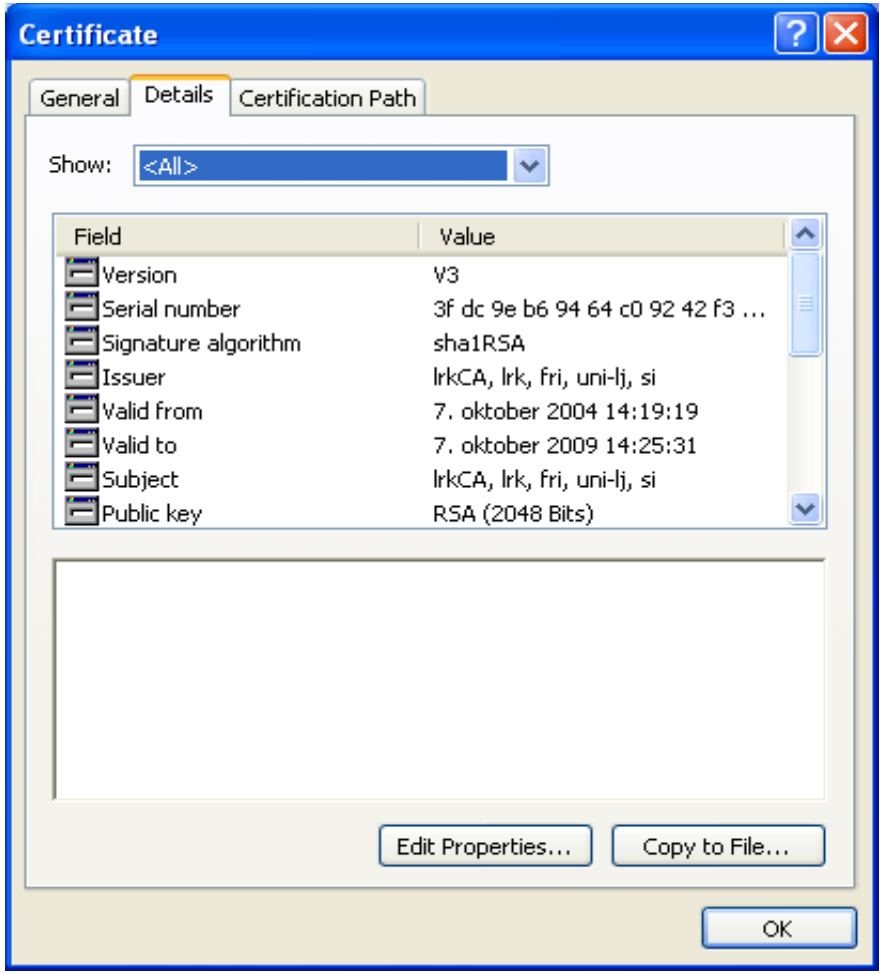
- ITU-T: International Telecommunication Union – oddelek za standardizacijo
- IETF- Internet Engineering Task Force (odprti standardi ,...)

Upravljanje z javnimi ključi

- Distribucija javnega ključa prek spleta (brez CA): napad s prestrezanjem - man in the middle
- CA
  - Garantira, da ključ pripada določeni entiteti.
- Certifikat (digitalno potrdilo):
  - Podatki o lastniku
  - Javni ključ
  - Ostali podatki
  - **Izvleček in podpis s strani CA**

Certifikat - primer

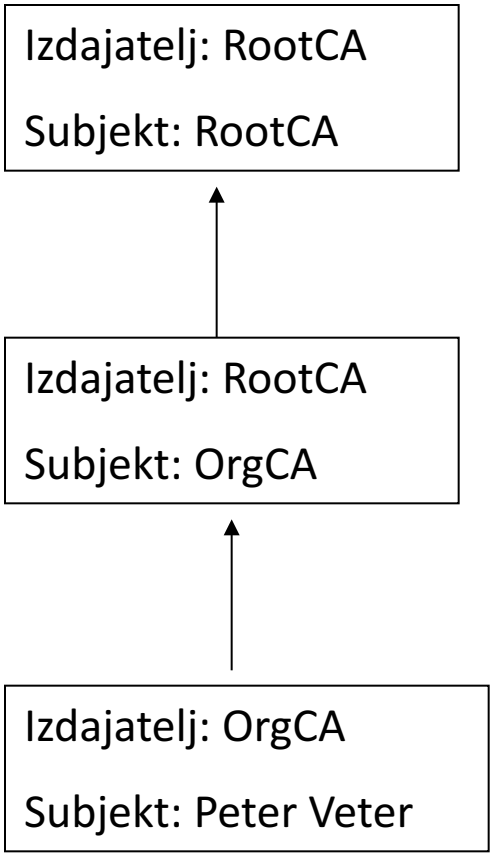




Preverjanje certifikata

- Izdajatelj CA
- Preverimo lahko
  - Integriteto certifikata
  - Identiteto lastnika
  - Z izdajateljevim javni ključem preverimo podpis certifikata
- Veriga zaupanja!

Veriga zaupanja



- Korenska avtoriteta
- Organizacijska CA
- Uporabnik

Veriga zaupanja

- Na vrhu je avtoriteta, ki ji eksplicitno zaupam.
- Samo-podpisan certifikat; varovanje!
- Eksplicitno lahko zaupamo tudi komurkoli nižje v verigi.

Veriga zaupanja

- Komu zaupata oba? Nikomur ?
  - Par novih certifikatov, vsakomu iz druge hierarhije
  - Navzkrižno certificiranje (CA)

Križno certificiranje

Izdajatelj: Root3CA

Subjekt: Root3CA

Izdajatelj: Root4CA

Subjekt: Root4CA

Izdajatelj: Root1CA

Subjekt: Org1CA

Izdajatelj: Root2CA

Subjekt: Org2CA

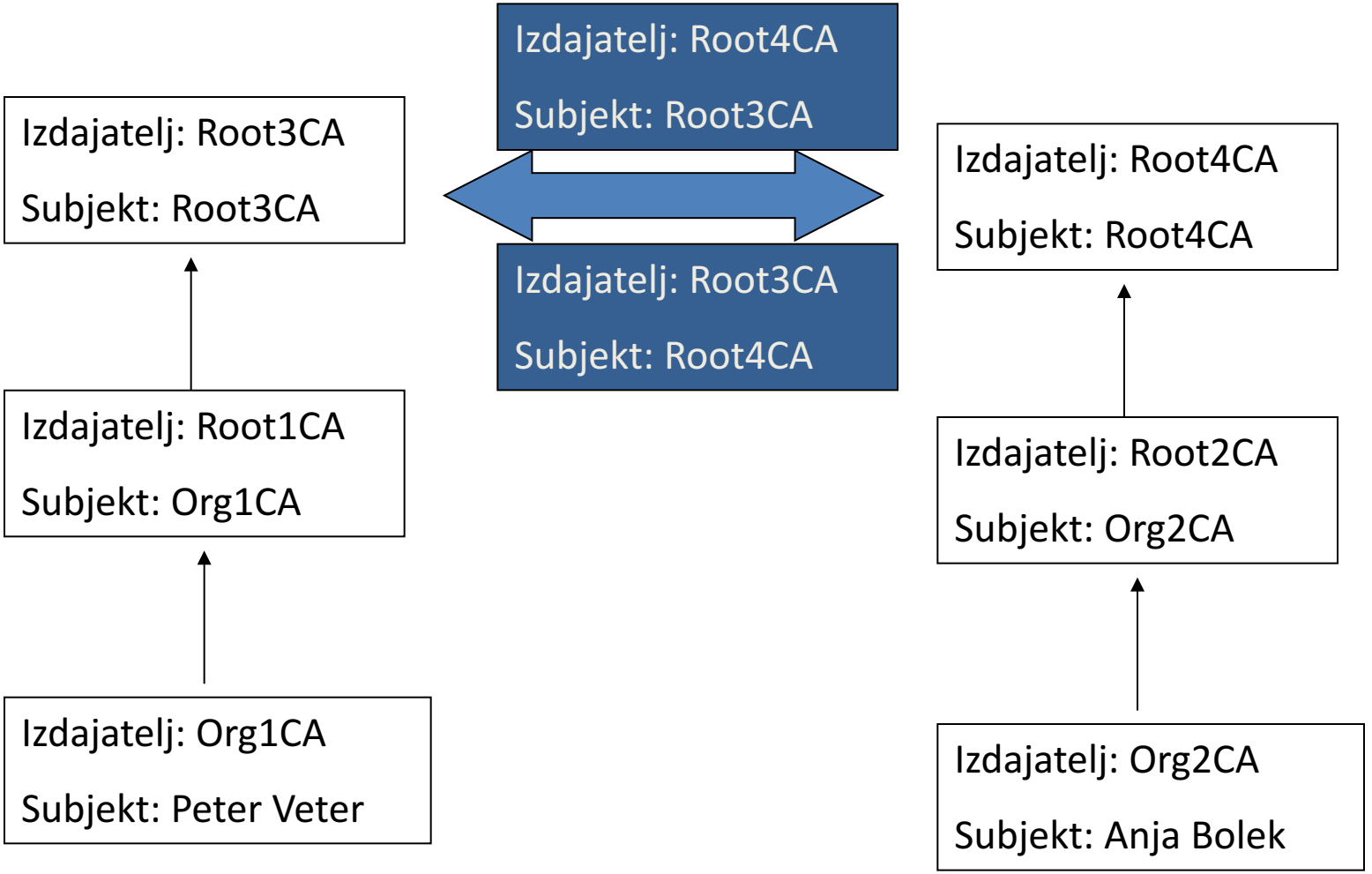
Izdajatelj: Org1CA

Subjekt: Peter Veter

Izdajatelj: Org2CA

Subjekt: Anja Bolek

Križno certificiranje



CRL - ČRNA LISTA

- Certificate Revocation List
- Sporne certifikate je potrebno preklicati! Npr. če
  - Ukraden
  - Menjava službe
  - Tajni ključ ogrožen
- CRL: podpis CA in čas (veljavnost)
- ARL – Authority Revocation List (koren)
- Validacija digitalnega potrdila: preveriti je treba tudi CRL (če ni bilo preklicano)!

PKCS –standardi (RSA lab.)

- PKCS #7 – Cryptographic Message Syntax (kako podpisati in kriptirati)
- PKCS #8 – Format shranjevanja ključa
- PKCS #10 – Format zahteve za certifikat
- PKCS #11 – Dostop do kripto naprave
- PKCS #12 – Zasebni ključi, certifikati, CRL

RFC

- RFC 3369 – Cryptographic Message Syntax
- RFC 3280 – X.509 PKI, certifikat in CRL profil.
- RFC 2315 = PKCS #7 – kako podpisati in kriptirati

Pregled celotne vsebine varnosti

- Kriptografija ☑
- Mehanizmi in protokoli (avtentikacija, integriteta...) ☑
- PKI ☑
- Omrežje – zgradba in požarne pregrade

Varna komunikacija

- Zaupnost – kdo sme prebrati? (enkripcija)
- Avtentikacija – dokaži, da si res ti,
- (Identifikacija – povej, kdo si - brez dokaza)
- Integriteta sporočila – je bilo med prenosom spremenjeno?
- Preprečevanje zanikanja (nonrepudiation) – res si poslal / res si prejel.
- **Razpoložljivost in nadzor dostopa** – preprečevanje nelegitimne rabe virov (avtorizacija – ugotavljanje, ali nekaj smeš storiti)

- Pomembno je tudi beleženje vseh dogodkov (dostopov, ...)

Protokola SSL (Secure Sockets Layer) in TLS (Transport Layer Security)

- Aplikaciji nudi varen kanal, overjanje strežnika in izmenjavo sejnih ključev.
- Leži nad transportno plastjo.
- Aplikacija se ga zaveda (zna uporabljati).
- Tipična uporaba:
  - na aplikacijski plasti za HTTP (https), FTP, SMTP, NNTP, SIP
  - Za tuneliranje celotnega omrežnega sklada – VPN nad transportno plastjo

Delovanje SSL/TLS

- Odjemalec: **ClientHello** (max. verzija TLS, naključno št., seznam podprtih kriptografskih p., izvlečkov in kompresij)
- TLS strežnik: **ServerHello** (izbrana verzija TLS, naključno št., izbrane metode iz seznama)
- TLS strežnik: svoje **digitalno potrdilo** [lahko tudi zahteva potrdilo od odjemalca]
- Odjemalec *lahko* preveri potrdilo.
- Na podlagi naključnih št. izračunata ključe.
- Komunikacija: simetrično kriptirana sporočila, dodan MAC (odtis sporočila)

Tipični algoritmi SSL/TLS

- Izmenjava ključev: RSA, Diffie-Hellman, PSK...
- Simetrično kriptiranje: RC4, 3-DES, **AES**, Camellia (starejši SSL: tudi DES, RC2, IDEA).
- Digitalni izvleček: MD5, SHA-1

IP Sec

- Nudi varen kanal na omrežni plasti
- Telo IP paketa se kriptira, glava pa ne (to bi onemogočilo usmerjanje).
- Dva protokola
  - Authentication Header protokol (AH) – nudi avtentikacijo izvora in integriteto podatkov, ne pa zaupnosti.
  - Encapsulation Security Protocol (ESP) – nudi avtentikacijo izvora, integriteto, in zaupnost.
  - V obeh se najprej ustvari varen logični kanal

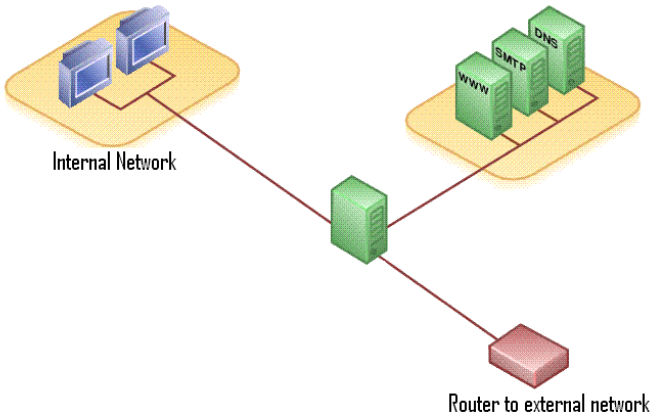
Nadzor dostopa: požarne pregrade

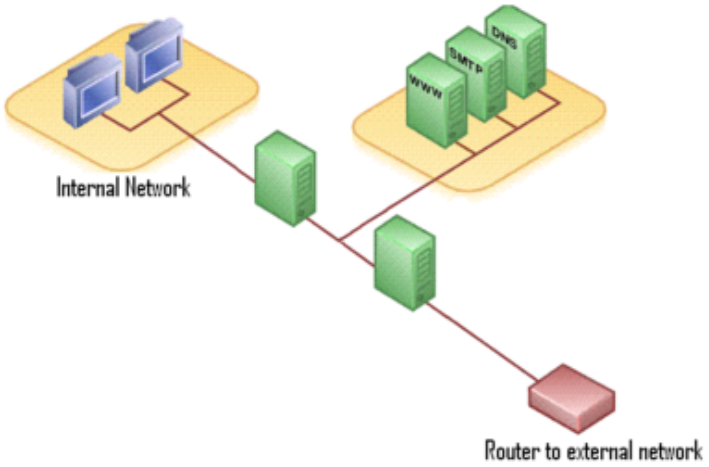
- Požarna pregrada: HW+SW, potreben za izolacijo med notranjim (zasebnim) in zunanjim (javnim) omrežjem.
  - **Paketno filtriranje**: na omrežni plasti gleda glavo paketa (IP številko, številko vrat – izvora in cilja)
  - **Aplikacijsko filtriranje**: gleda aplikacijska sporočila, (Deep packet inspection) – ne samo glavo.
- IDS (intrusion detection system)
- IPS = aktivni IDS (intrusion prevention system)
  - Vzorci ali podpisi napadov

DMZ

- Demilitarized zone
- Del omrežja, ki vsebuje infrastrukturo storitev, ki jih podjetje nudi javnemu (nevarnemu) internetu.
- Napadalec lahko dostopa le do DMZ, ne do celotnega omrežja
- Tipične storitve: spletni strežnik, poštni strežnik, posredniki (proxy) in obratni posredniki (reverse proxy) – aplikacijski požarni zid (posreduje pri dostopu v interno omrežje, npr. interni poštni strežnik)

Postavitev DMZ:
ena ali dve požarni pregradi





Napadi DoS in DDoS

- DoS napad povzroči, da sistemski viri niso več na voljo legitimnim uporabnikom. Primeri...
  - SYN flooding: napadalec vzpostavlja TCP sej (veliko število!), vendar rokovanja ne zaključi (strežnik ga čaka – porablja vire)
  - SMURF napad: podobno kot zgoraj. Napadalec iz hlinjenega naslova pošilja ping na več računalnikov, ti nato pošiljajo echo-reply na hlinjeni (napadeni) naslov.
- DDoS iz botneta: napadalec si podredi (vdre) večje št. računalnikov – sužnjev (botnet), podtakne jim svoj program. Na njegov ukaz vsi hkrati DoS-napadejo tarčo.

- Detekcija in obramba: zelo težko! Filtriranje prometa, detekcija vzorcev. Težko ločiti npr. legalen in nelegalen ping.

Napadi z družbenim inženiringom

- To so napadi na človekovo psiho
- Napadalec te prepriča, da ravnaš drugače, kot bi sicer
  - Nakažeš 5000 EUR v Nigerijo
  - Klikneš na povezavo, ki jo dobiš v mailu
  - Vpišeš geslo v spletni obrazec
  - Vpišeš številko kreditne kartice
  - Izvoziš zasebni ključ in ga pošlješ po mailu
- Danes predstavljajo pomemben del napadov. Vedno težje jih razpoznamo, težko je tudi preprečevanje.

Varnostni standardi

- ISO/IEC 27000 serija (prej 17799 ter BS 7799) :
  - ISMS – Information Security Management System
  - najboljše prakse z nadgradnjo
  - osnova certificiranja
- Slovenske različice (SIST)
  - Sistemi za upravljanje varovanja informacij – Specifikacija z napotki za uporabo
  - Informacijska tehnologija – Kodeks upravljanja varovanja informacij

ISO/IEC 27002:2013
Sistem upravljanja varovanja informacij
Information technology — Security techniques — Code of practice for information security controls

- 14 bistvenih poglavij - področij, za vsako so določeni cilji, vsak cilj nadziramo s pomočjo kontrolnih točk (nadzorstev).
  - skupno 35 ciljev,
  - 114 nadzorstev

Primeri poglavij, ciljev, kontrol

- Fizična zaščita in zaščita okolja
  - Varovana območja
    - kontrole fizičnega dostopa (npr. beležimo čas prihoda in odhoda, identifikacija z magnetno kartico)
  - Varovanje opreme
    - Namestitev in zaščita pred krajo, ognjem, prahom…
    - Oskrba z energijo (UPS, generator)
- Upravljanje z operacijami
  - Zaščita pred zlonamerno programsko opremo
    - Namestitev in posodabljanje protivirusnih programov…
  - Beleženje in nadzor
    - Aktivnost uporabnikov, adminov, napake, incidenti...
  - Upravljanje s tehničnimi ranljivostmi
    - Nameščanje popravkov in novih različic; kaj lahko nameščajo uporabniki sami
- Varnost komunikacij
- Šifriranje