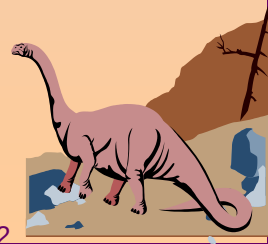
Varnost

- Pri komuniciranju preko računalniške mreže se pojavijo vprašanja v povezavi z varnostjo in zasebnostjo.
- Zelo velika omrežja, kot je internet, so ranljiva za napade. Nihče interneta ima pod nadzorom.
- Paketi se pogosto pošiljajo nezaščiteni.
- Napadalec lahko prebere sporočilo (e-pošto) pri njeni poti skozi omrežje MTAjev.
- Napadalec lahko ponaredi identiteto pošiljatelja; pošilja pošto v tujem imenu.
  - ☞ To je zelo enostavno narediti; na vrata 25 MTAja je potrebno le poslati nekaj ukazov SMTP.
- V sporočila s priponkami je mogoče podtakniti priponke s škodljivo vsebino – viruse, črve…
- Napadalec je lahko kdorkoli; iz druge države, bivši zaposleni, zaposleni v istem podjetju…

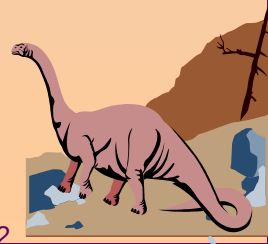


Vrste napadov

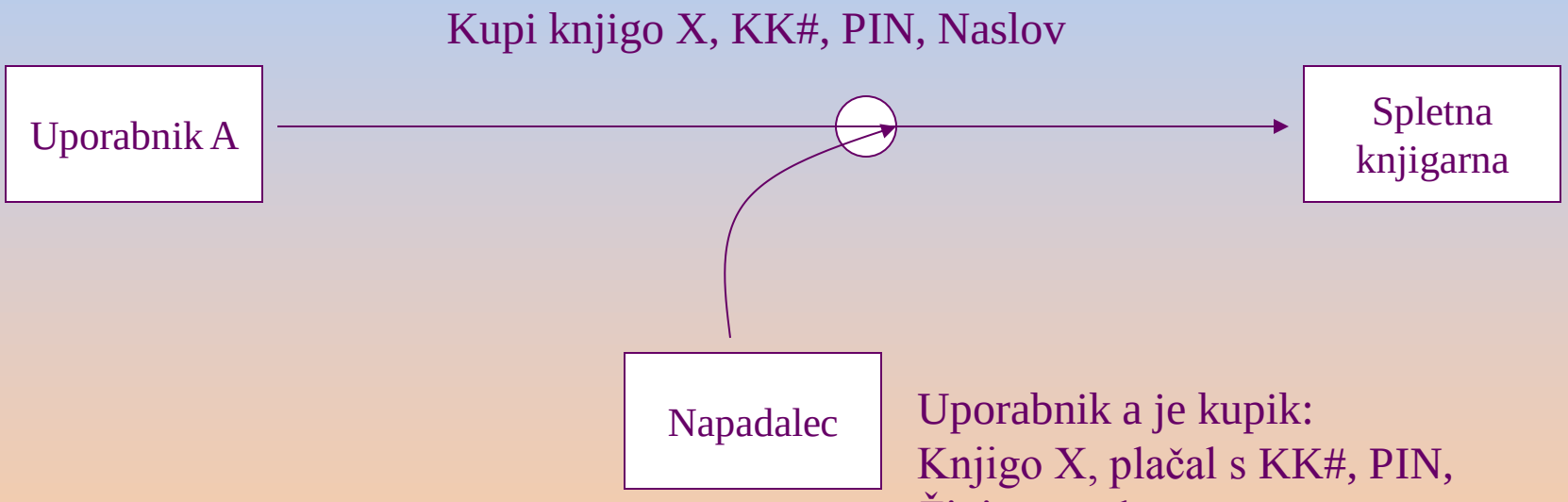
- **Pasivni napad** (podobno kot prisluškovanje telefonskim pogovorom)
- Na ta način napadalec pride do informacij, ki jih kasneje lahko uporabi.
- Npr. podatki o kreditni kartici.
- Take napade je praktično nemogoče zaznati.

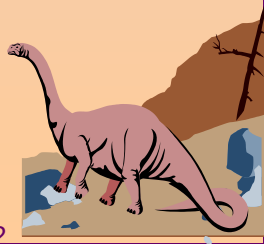
- **Aktivni napad** v primeru, ko napadalec spreminja ali podvaja podatke

nezaščiten komunikacijski kanal

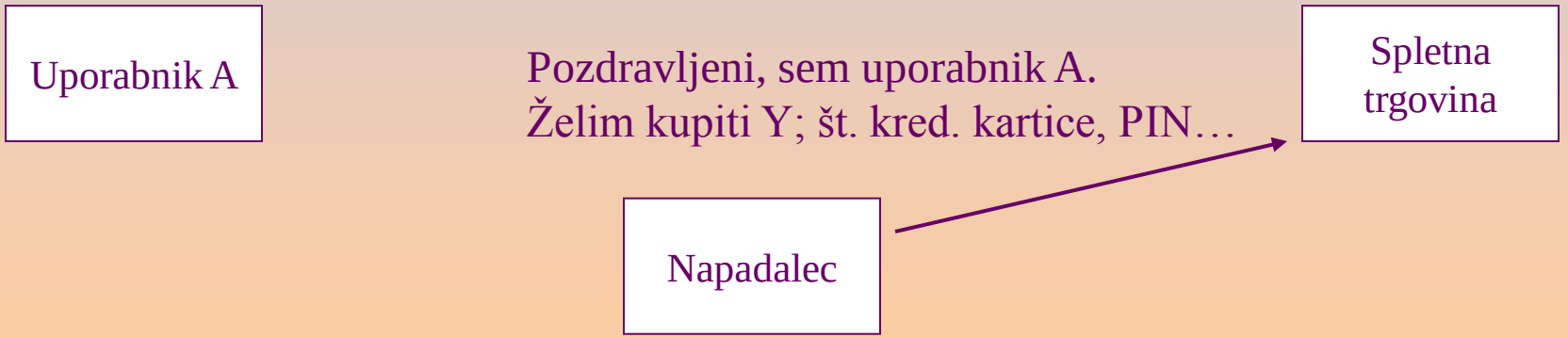


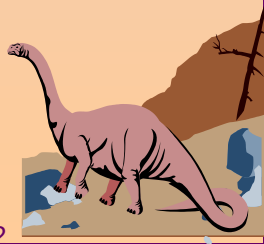
- Vrste napadov
  - **Prisluškovanje** (pasivni napad)
  - Napadalec pridobi kopije sporočil
  - To se doseže s pregledovanjem prometa po mreži



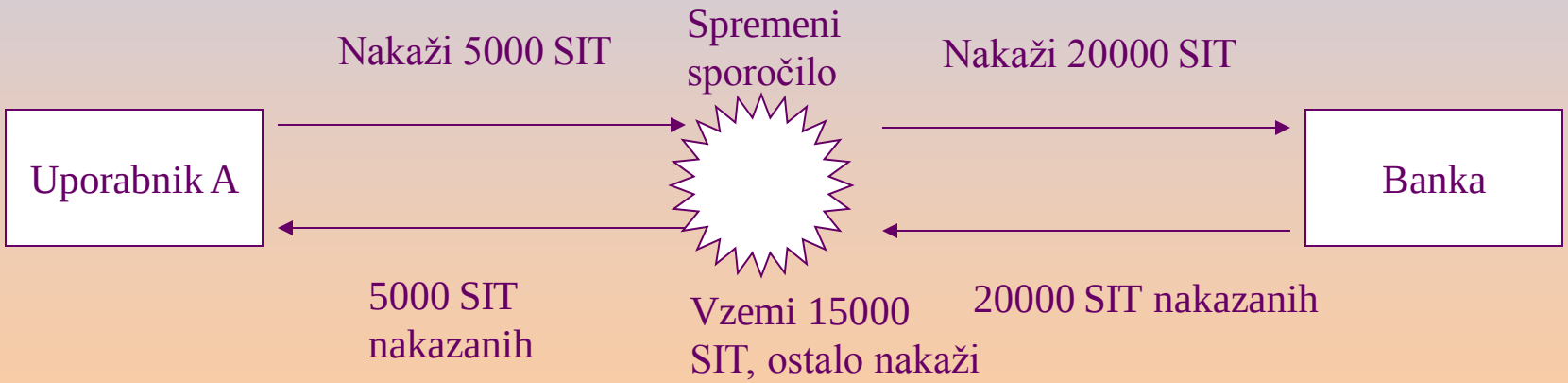


- Vrste napadov
  - **Prevzem identitete**
  - Pošiljanje ali sprejemanje sporočil v imenu napadenega; pri tem se uporabi lažna identiteta, ukradeni podatki… Kako? Kraja gesel, PINov,št. kreditnih kartic, drugih podrobnosti s prisluškovanjem.
  - Uporaba pridobljenih podatkov…



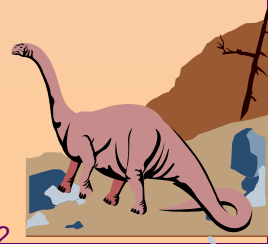


- Vrste napadov
  - **Spreminjanje sporočil**
  - Prestrezi sporočilo in ga spremeni
  - Spremenjeno sporočilo pošlji pravemu naslovniku
  - Vključuje:
    - Določene zamenjave podatkov, brisanje podatkov
    - Kreiranje drugačnega sporočila



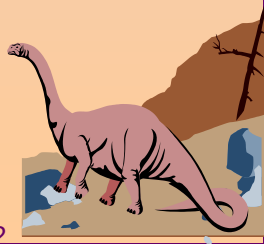
Kriptiranje

- Enkripcija
  - Kodiranje podatkov na tak način, da jih lahko *dekriptira* samo tisti, ki ima **ključ**
  - Poznana že iz rimskih časov
- Simetrično kriptiranje
  - Pri enkripciji in dekripciji se uporablja isti ključ
  - Ključ poznata samo pošiljatelj in naslovnik
  - Težave z distribucijo ključa
  - Hitri postopki
- Nesimetričn kriptiranje (javni ključ)
  - Dva ključa E-enkripcija, D-dekripcija
  - E – **javni ključ**; pozna ga lahko ‘vsakdo’
  - D – **zasebni ključ**; pozna ga samo lastnik
  - Počasni, zapleteni postopki



Kriptiranje

- Simetrično kriptiranje
  - E=D=E
  - P→E(P)…→E(E(P))
  - Data Encryption Standard (DES), Tripe-DES (3DES), International Data Encryption Algorithm (IDEA), SAFER, Blowfish
- Nesimetrično kriptiranje
  - P→E(P) … →D(E(P))
  - Rivest, Shamir, and Adleman (RSA), Digital Signature Standard (DSS), Elliptic Curve Cryptography (ECC)

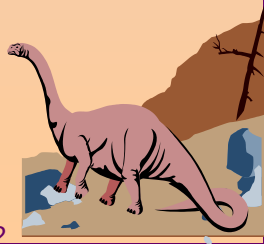


Kriptiranje – RSA

- Izberemo p,q: veliki praštevili, npr. 1024 bitov
  - $n = pq$
  - $z = (p-1)(q-1)$
- Izberemo d: nima skupnih deliteljev s številom z.
- Izberemo e: $ed \bmod z = 1$

- $P \rightarrow C=P^e \bmod n$ *kriptiranje; E = (e, n)*
- $C \rightarrow P=C^d \bmod n$ *dekriptiranje; D = (d, n)*

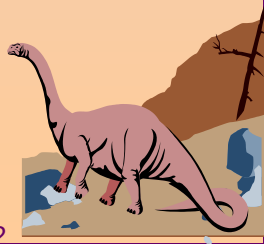
- *Razbijanje kode: n poznan; zelo težko ugotovimo p in q*



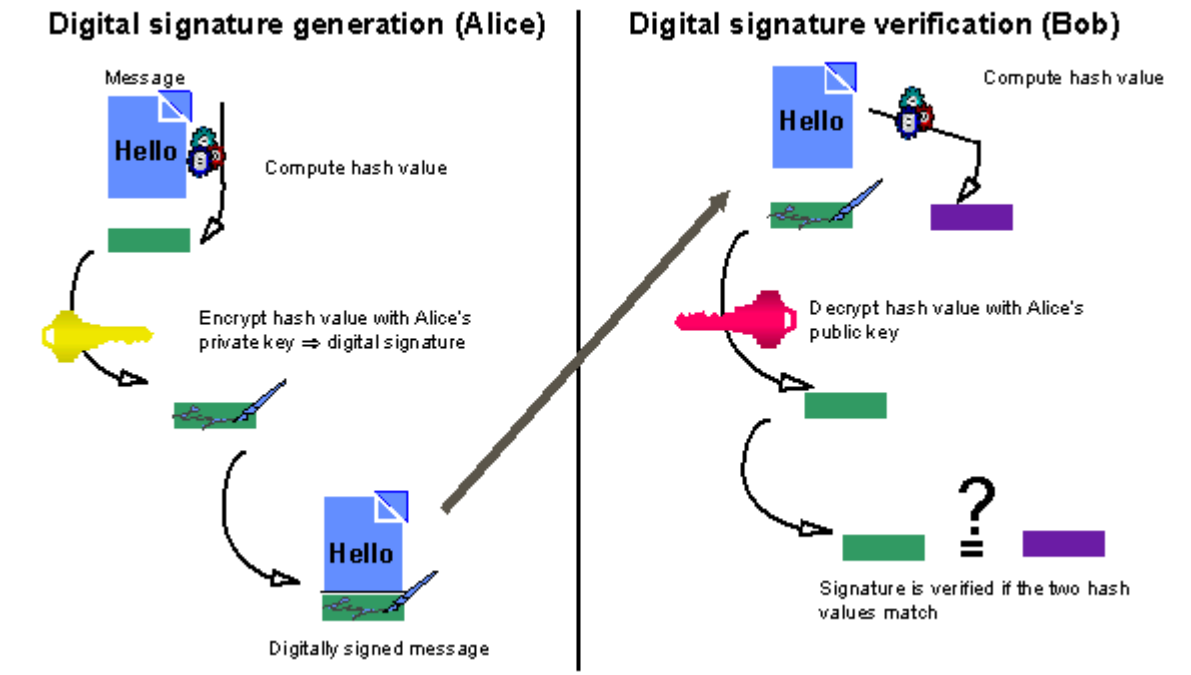
Kriptiranje – zgled RSA

- p = 3, q = 11
- n = 33, z = 20
- d = 7, e = 3
- P $\rightarrow$ $C=P^3$ mod *33* *enkripcija*
- C $\rightarrow$ $P=C^7$ mod *33* *dekripcija*

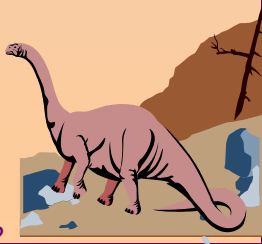
	P	P^3	C	C^7	$C^7 \bmod 33$
T	21	9261	21	1801088541	21
E	06	216	18	612220032	06
K	12	1728	12	35831808	12
S	19	6859	28	13492928512	19
T	21	9261	21	1801088541	21



Elektronski podpis



- Hash – povzetek sporočila
  - Majhna verjetnost, da imata različni sporočili enako hash vrednost
- Kriptiraj hash vrednost z zasebnim ključem
- Pošlji
- Sprejemnik ponovno izračuna hash vrednost
- Dekriptiraj sprejet elektronski podpis
- Primerjaj hash vrednosti; preveri ujemanje
- Možno, če E(D(P)) = D(E(P))



Kriptiranje - SSL

- Secure Socket Layer
- Simetrično kriptiranje na transportnem sloju
- Delovanje:
  - Odjemalec pošlje strežniku podatke o podprtih načinih kriptiranja
  - Strežnik pošlje odjemalcu svoj **javni ključ.**
  - Odjemalec generira naključni ključ, ki se bo uporabljal v seji, ga kriptira s strežnikovim javnim ključem in pošlje strežniku.
  - Vzpostavi se varna povezava, podatki se kriptirajo z dogovorjenim ključem
  - Ključ velja za čas ene seje.