Varne komunikacije

Anton Umek
anton.umek@fe.uni-lj.si

Laboratorij za komunikacijske naprave

Veda o šifriranju

Šparta, 500 p.n.š.

KRIPTOGRAFIJA: kriptos logos

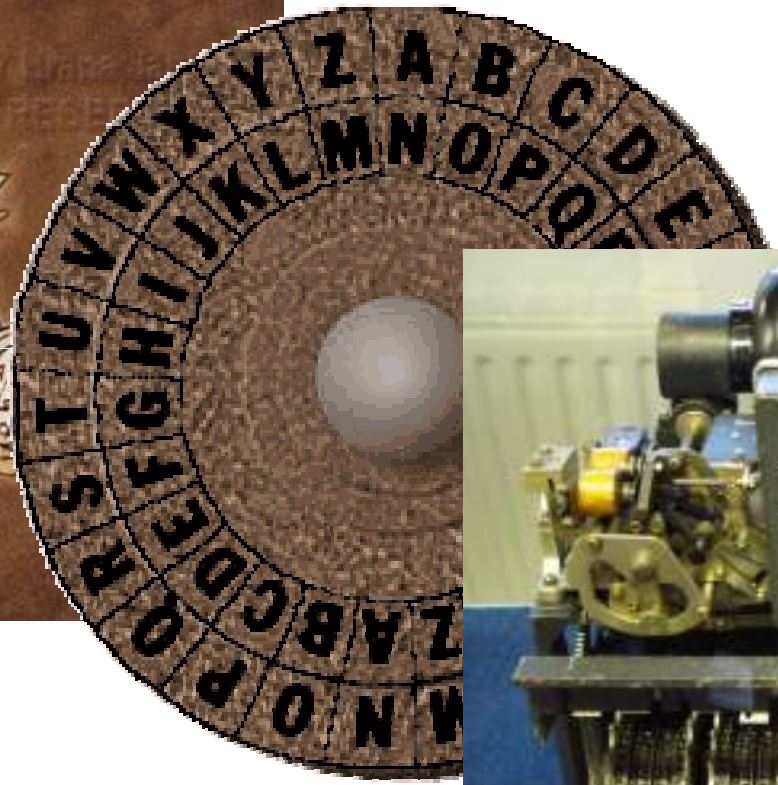
Veda o šifriranju

Šparta, 500 p.n.š.

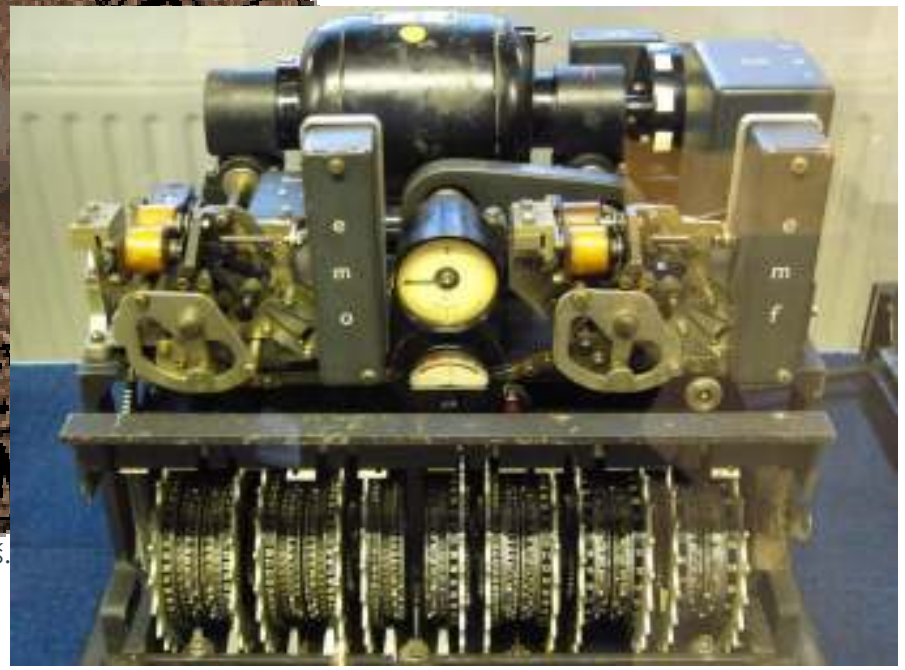
Julij Cezar, 100 p.n.š.

Veda o šifriranju

Šparta, 500 p.n.š.



Julij Cezar, 100 p.n.š.



Enigma, 1920-1940

Moderno šifriranje

- šifrirni **algoritem je javen**, varnost temelji na tajnosti ključev !

- **namen** šifriranja, varnostni vidiki:
  - tajnost
  - verodostojnost
  - avtentičnost
  - neovrgljivost

- šifrirni **algoritmi**:
  - DES, IDEA, **AES**
  - **RSA**, DH
  - MD5, SHA-1,..SHA-3

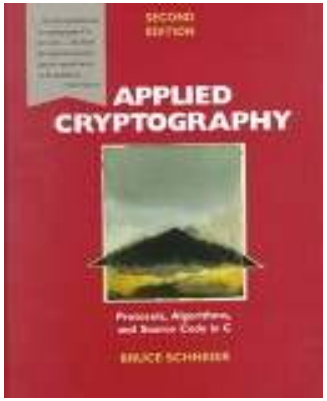
Kriptoanaliza – razbijanje šifer

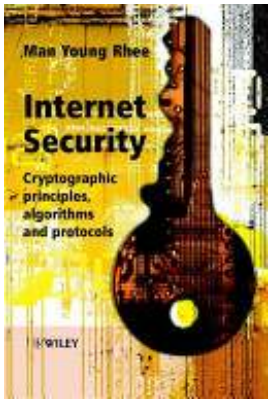
Varnost radijskih komunikacij

Varnost komunikacij na Internetu

Študijsko gradivo

- http://www.lkn.fe.uni-lj.si/gradiva/Varne_komunikacije/
- Glavni vir in priporočena literatura za poglobitev znanja:






Varne komunikacije
izbirni modul D

Vsebina

- Zgodovina šifriranja, razvrstitev sodobnih šifrirnih algoritmov.
- Analiza standardnih šifrirnih algoritmov s primeri uporabe v praksi.
- Standardne zgoščevalne funkcije in digitalni podpis.
- Digitalni certifikati in infrastruktura javnih ključev.

- Varnost komunikacij na Internetu s pregledom mehanizmov varovanja na različnih plasteh.
- Varnost komunikacij v radijskih sistemih (GSM, TETRA, UMTS, WLAN).
- Varnostna politika in upravljanje varnosti v komunikacijskem sistemu.

Pridobljena znanja:

- Prepoznava osnovnih vidikov varnosti: tajnost, avtentičnost, verodostojnost, in neovrgljivost.
- Razumevanje temeljnih principov varovanja informacij v komunikacijskih sistemih.
- Pridobitev temeljnih znanj o varnostnih mehanizmih in praktičnih znanj o varnostnih protokolih, ki se uporabljajo na Internetu in v mobilnih radijskih omrežjih.

Varnost ima vse večji pomen

- Kaj imate vedno pri sebi, je novinarje pred petimi leti na veliki telekomunikacijski konferenci vprašal predstavnik vodilnega izdelovalca mobilnih telefonov.
- Denarnico, ključe in mobilnik, je odgovoril.
- Ko bom vprašanje ponovil čez nekaj let, o denarnici in ključu ne boste več razmišljali. Ostal bo samo še mobilnik…