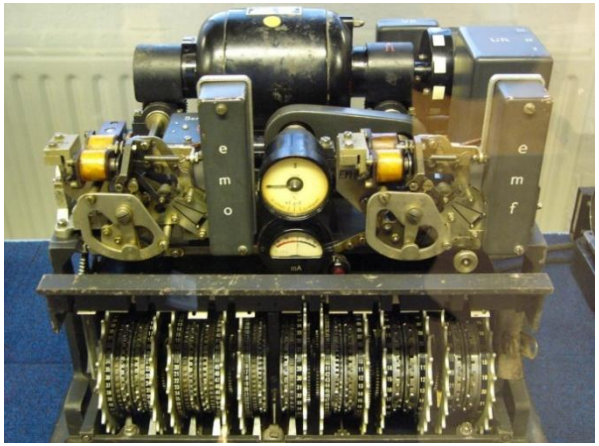
Varne komunikacije

viš. pred. dr. Anton Umek

Univerza *v Ljubljani*
Fakulteta *za elektrotehniko*

Zgodovina vede o šifriranju

- Šifrirni algoritmi so bili dolgo časa strogo varovana skrivnost:



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

Varnost komunikacij

- na internetu,
- radijske zveze in
- mobilni internet

Vsebina predmeta

- 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 (WLAN , GSM, TETRA, UMTS, LTE).
- Varnostna politika in upravljanje varnosti v komunikacijskem sistemu.

Cilji in pridobljena znanja

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

Študijsko gradivo

- Dopolnilno gradivo za poglobitev znanj:
  - Bruce Schneier: Applied Cryptography,
  - Man Young Rhee: Internet security,