

**Suvisiace predmety so ZKRY**

# ŠKS (1.Ing LS)

- Protokoly na vymenu kluca (Kerberos protocol, TLS, ...)
- End-to-end encryption (Signal protocol, ...)
- Blind signatures
- Commitment schemes
- Secret-sharing schemes
- Zero-knowledge proofs
- Secure multi-party computation
- ...

# NKŠ (2.Ing ZS)

- Navrh a kryptoanalyza sifier.
- Predmet uci prof. Pavol Zajac.

# Teoria kodovania (2.Ing ZS)

- Predmet uci pani Cipkova.