Criptografia 2016/17

Criptografia simétrica ou de chave privada

- Técnicas base: substituição e transposição
- Shift de César
- Bastão – antigo Egipto
- Cifra de Vigenère (substituição polialfabética)
- 1ª guerra mundial: protocolo ADFGVX
- 2ª guerra mundial: máquina Enigma
- DES e AES

Segurança de sistemas criptográficos

- Princípio de Kerckhoff

Criptografia assimétrica ou de chave pública

- DLP – o problema do logaritmo discreto
- O protocolo de Diffie-Hellman para partilha de chaves
- Método "rápido" de cálculo de potências (fast powering algorithm)
- O pequeno teorema de Fermat
- O teorema de Euler
- RSA
- Ataques ao RSA

Extra (não avaliado em teste/exame)

- Partilha de chaves (com e sem limiar)
- Curvas elípticas
- Protocolo de Diffie-Hellman sobre curvas elípticas