CRYPTOGRAPHY

MESIGI3906
HASH FUNCTIONS AND MAC

JOHN CAGNOL / AMAURY DARSCH
DER CALCUL SCIENTIFIQUE / DER GÉNIE INFORMATIQUE

AGENDA

- Hash functions with OpenSSL
  - MDX familly
  - SHA familly
- Message authentication code
  - HMAC

TESTING FOR MD5

- Unix command
  - `md5sum [file]`
- OpenSSL command
  - `openssl dgst -md5 -hex [file]`
- Example
  - `Message:LEONARDO DA VINCI`
  - `b17e05ba4e954b5818a25e36be4b6c76`

TESTING FOR SHA

- Unix command
  - `sha1sum [file]`
- OpenSSL command
  - `openssl dgst -sha1 -hex [file]`
- Example
  - `Message:LEONARDO DA VINCI`
  - `512835032a5ea0bcec91621ef5b236096778ed9c`
- Other commands
  - `Sha256sum, sha384sum, sha512sum`
  - Also available with OpenSSL

MAC

- Message authentication code
  - A code that authenticates a message
  - Must be unique for a given message
  - Must be protected by a key
- HMAC
  - Hashed mac
  - Standard – FIPS PUB 198
  - HMAC(K, m) = h (K ⊕ opad || h (K ⊕ ipad || msg))
- Not available in OpenSSL as a command