7.5 hp, Spring term 2008

Network Security

Lecture 2

Asymmetric ciphers

Message authentication

Kristina.Kunert@hh.se

Message authentication

- Use of MAC and hash functions
- Public-key encryption principles
- Public-key encryption to produce digital signatures
- Key management

- Authentic → genuine, from alleged source
- Authentication → verify unaltered contents, verify that source is authentic
- Plus: timeliness, sequence
- Possible to use symmetric encryption
  - Plus error-detection code, sequence number, timestamp

Secure hash function

- Requirements
  - Input data block: any size, Output: fixed length
  - H(x) easy to compute for all x
  - One-way property, Weak & String collision resistance

Simple hash function

- Input: sequence of *n*-bit blocks
- Input processed iteratively one block at a time → *n*-bit hash fcn
  - E.g. Bit-by-bit exclusive-OR (XOR)

MAC

- $MAC_M = F(K_{AB}, M)$

One-way hash function

- Using conventional encryption, using public-key encryption or using secret value

SHA-512

- SHA-512
  1. Append padding bits
  2. Append length
  3. Initialize hash-buffer
  4. Process message in 1024-bit blocks
  5. Output
- MD5: questionable security
- Whirlpool: Block cipher in compression fcn
- HMAC: Secret key in hash fcn

Public-key cryptography

- Ingredients
  - Plaintext, Encryption algorithm, Public and private key, Ciphertext, Decryption algorithm
- Applications
  - En-/Decryption, Digital signature, Key exchange
- Algorithms
  - RSA
    - Block cipher
    - $C=M^e \bmod n$
    - $M=C^d \bmod n$
  - Diffie-Hellman
    - Key exchange algorithm only