Lab 12 - Securitate

Criptare simetrica

- o singura cheie C
- C(M) = MC
- C(MC) = M
- AES, DES, IDEA, RC5, Blowfish, Twofish
- greu de gestionat stabilirea cheii partajate

Criptare asimetrica

- doua chei: publica (E), privata (D), D(E(M)) = M = E(D(M))
- A vrea sa ii trimita un mesaj M lui B:
  - cripteaza cu cheia publica a lui B: $E_B(M)$
  - B decripteaza cu cheia sa privata: $D_B(E_B(M)) = M$
- RSA
- un atacator de tip man-in-the-middle (MITM) poate sa preia mesajul, sa il modifice, apoi sa il recripteze cu E_B

Rezumate de mesaje si semnaturi digitale

- rezumat/digest = sir de biti de lungime fixa, generat cu ajutorul unei functii de hash MD
- se foloseste la verificarea transmisiei corecte → un MITM poate prelua mesajul si il poate modifica (cu tot cu rezumat)
- solutia → utilizarea semnaturilor digitale:
  - A vrea sa ii trimita un mesaj M lui B
  - A calculeaza rezumatul mesajului: MD(M)
  - A cripteaza rezumatul cu cheia sa privata: $D_A(MD(M))$
  - A trimite mesajul M si $D_A(MD(M))$
  - B decripteaza rezumatul cu cheia publica a lui A: $E_A(D_A(MD(M))) = MD(M)$
  - B verifica daca MD(M) este corect
- MD5, SHA-1, SHA-2, SHA-3

Certificate

- identitatea si cheia publica a solicitantului, semnate digital
- oferite de o CA (Certification Authority)
- X.509

Link-uri

[Lab OCW]
[SSH handshake]
[TLS handshake]
[Formular feedback]
[C Crash Course]
[Guide to Network Programming]