Crittografia Oggi

Programma del corso

1. Introduzione alla crittografia
   a) confidenzialità, autenticità, integrità
   b) principi ed ingredienti
   c) cifrario di Cesare e One-Time-Pad
   d) principio di Kerchoff
   e) crittoanalisi
   f) tipi di algoritmo: simmetrici, a-simmetrici, di hash
2. Algoritmi simmetrici
   a) a blocchi e a stream
   b) principali algoritmi simmetrici
   c) DES
   d) AES
3. Algoritmi A-simmetrici
   a) principi generali
   b) introduzione a RSA
   c) uso delle chiavi pubbliche e private
4. Algoritmi di hash
   a) principi di un algoritmo crittografico di hash
   b) MAC e H-MAC
   c) da MD5 e SHA1 a SHA-256 ecc.
5. Protocolli crittografici
   a) confidenzialità
   b) autenticità
   c) integrità
   d) uso combinato degli algoritmi

6. OpenPGP
   a) Il protocollo OpenPGP
   b) web of trust
   c) gestione delle chiavi
   d) formato dei documenti firmati e/o cifrati
   e) esempi di uso [dimostrazioni pratiche]
   f) la posta elettronica e OpenPGP
7. Certification Authority e Openssl
   a) i certificati digitali
   b) creare una CA con Openssl
   c) creare certificati con Openssl
   d) esempi di uso [dimostrazioni pratiche]
   e) usare un certificato digitale per la navigazione web
   f) effettiva sicurezza della navigazione web protetta da PKI