Sistemi di elaborazione dell'informazione: Sicurezza su reti
PROF. ALFREDO DE SANTIS — Anno Acc. 1997-98

Programma del corso

Crittografia Classica.
Data Encryption Standard (DES) e modalità operative.
DES triplo.
Cifrari a blocchi (IDEA, RC5).
Distribuzione di chiavi (Blom, Kerberos, Needham-Schroeder).
Accordo su chiavi (Diffie-Hellman, puzzle di Merkle).
Crittografia a chiave pubblica (RSA, Rabin, El Gamal, Merkle-Hellman, Mc Eliece).
Firme digitali (RSA, ElGamal, Digital Signature Standard, Lamport, Bos-Chaum).
Funzioni hash (MD4, MD5, SHS).
Certificazione del tempo.
Autorità di certificazione.
Autenticazione (password, S-key).
Schemi per la condivisione di segreti.
Crittografia Visuale.
Schemi di identificazione (Schnorr, Guillou-Quisquater).
Zero-knowledge.
Protocolli sicuri (Poker mentale, Lancio di Moneta, Oblivious Transfer, Firme di Contratto, Protocollo del Milionario, Elezioni, Key Escrow, Fair Cryptoystem).
Moneta elettronica. Protocollo iKP.
Pretty Good Privacy (PGP).
Tecniche biometriche di identificazione.
Protezione della proprietà intellettuale.
Virus.

La maggior parte del materiale del corso si puó trovare nei seguenti libri:

1. Doug R. Stinson, Cryptography: Theory and Practice, CRC Press Inc., 1995.
2. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Second Edition, 1996.
3. W. Stallings, Network and Internetwork Security, IEEE Press 1995.

Gli appunti delle lezioni si trovano ad http://www.unisa.it/CorsoSecurity/
(oppure su [zoo]/pub/src/gnu/security/www).