Teoria dell'Informazione / Crittografia

Prof. Giancarlo Mauri / Dott. Alberto Leporati

Dipartimento di Informatica, Sistemistica e Comunicazione (DISCo)
Università degli Studi di Milano - Bicocca
Via Bicocca degli Arcimboldi 8, 20126 Milano

Programma dettagliato

- **Introduzione:** schema di un sistema di trasmissione (Alice, Bob, Eve) e applicazioni della crittografia. **Definizioni:** spazio dei messaggi in chiaro, dei messaggi cifrati e delle chiavi. Definizione di crittosistema.
- **Sistemi di cifratura monoalfabetici:** sistemi a sostituzione e a trasposizione. Crittosistema di Cesare, crittosistema di Hill basato sull'algebra lineare. Crittoanalisi: analisi delle frequenze. Crittosistemi monoalfabetici con nulle e omofoni.
- **Sistemi di cifratura polialfabetici:** Playfair. Crittoanalisi: digrammi. Sistema di Vigenère e sua crittoanalisi. Rotori e DES. One-Time Pad.
- **Generatori pseudocasuali, predicati hard-core e hard-core bits.** Funzioni one-way: problema del logaritmo discreto, fattorizzazione. Costruzione di generatori pseudocasuali. Teorema di Goldreich-Levin sulla costruzione di predicati hard-core.
- **Crittosistemi a chiave pubblica:** L'idea della chiave pubblica (cassette di sicurezza con due lucchetti) e sua formalizzazione. Esempio: crittosistema di El Gamal. Crittosistemi ibridi. Scambio delle chiavi di Diffie-Hellman.
- **RSA.** Funzionamento di RSA. Test di primalità. Scelta dei parametri. Alcuni semplici attacchi.
- **Sistemi di prova interattivi Zero-Knowledge**. Due definizioni alternative di NP. Sistemi di prova interattivi. Esempio: il linguaggio NONISO. Sistemi di prova interattivi zero-knowledge: definizione ed esempio per il linguaggio ISO.
- **Cenni sulle applicazioni:** commercio elettronico (SSL), smartcard, VPN (Virtual Private Networks)(IPsec), PGP.