Parole chiave del modulo di crittografia

- Cos'è la crittografia - Storia della crittografia
- Probabilità Discreta - One Time Pad e sicurezza perfetta di Shannon
- Stream Ciphers and Pseudo Random Generators
- Attacks on Stream Ciphers and The One-Time Pad
- Real-World Stream Ciphers (uno weak(RC4), e eStream,nonce, Salsa20)
- Cenni di sicurezza semantica
- Cifrari a blocchi, DES
- Exhaustive Search Attacks per i cifrari a blocchi
- AES, Block Ciphers From PRGs
- Mode of Operations: One time key
- Security for Many-Time Key (CPA Security)
- Modes of Operation: Many Time Key (CBC)
- Key Exchange:
- Trusted 3rd Parties
- Merkle Puzzles, The Diffie-Hellman Protocol
- Aritmetica Modulare
- Public key encryption: definitions and security
- (pub-key) Chosen Ciphertext Security
- Trapdoor Permutations
- Hash Function
- Public key encryption
- RSA: Attack on textbook RSA, Is RSA a one-way function? , RSA in practice
- Digital Signatures
- ElGamal