Elementi di Crittografia

Programma del corso

A.A. 2023/2024

Prof. Paolo D'Arco

Introduzione	**Capitolo 1**
Cifratura perfettamente segreta	**Capitolo 2 (2.1 – 2.3)**
Cifratura a chiave privata	**Capitolo 3**
Codici per l'autenticazione dei messaggi	**Capitolo 4 (4.1 – 4.5)**
CCA-Security e cifratura autenticata	**Capitolo 5**
Funzioni hash ed applicazioni	**Capitolo 6 (escluso 6.4.3)**
Costruzioni pratiche di primitive simmetriche	**Capitolo 7 (escluso 7.2.6)**
Costruzioni teoriche di primitive simmetriche	**Capitolo 8 (vedi slide)**
Teoria dei numeri e assunzioni crittografiche	Appunti/slide o **Capitolo 9**
Gestione delle chiavi e rivoluzione a chiave pubblica	**Capitolo 11**
Cifratura a chiave pubblica	**Capitolo 12**
Firme Digitali	**Capitolo 13 (fino a 13.5)**
Secret sharing (cenni)	**Vedi slide**
Sistemi di prova a conoscenza zero (cenni)	**Vedi slide**

I teoremi principali da rivedere sono (per i teoremi in **grassetto** le prove sono nel ROM):

Thm 2.11 (shannon bound)

Thm 3.16 (encryption con PRG) Thm 3.29 (encryption con PRF)

Thm 6.4 (Merkle Damgard transform)

Thm 9.79 (hash collision-resistant) Thm 11.3 (Diffie-Hellman protocol)

Thm 12.18 (El Gamal encryption) **Thm 12.21** (El Gamal KEM)

Thm 12.31 (RSA encryption – one bit) **Thm 12.38** (KEM RSA)

Thm 13.7 (RSA-FDH – sketch, come a lezione)