

# INGEGNERIA INFORMATICA (LM75)

(Lecce - Università degli Studi)

## Insegnamento SICUREZZA DEI SISTEMI

GenCod A006803

Docente titolare Francesco TOMMASI

Insegnamento SICUREZZA DEI SISTEMI Anno di corso 1

Insegnamento in inglese SYSTEMS SECURITY

Lingua ITALIANO

Settore disciplinare ING-INF/05

Percorso PERCORSO COMUNE

Corso di studi di riferimento INGENGERIA INFORMATICA

Tipo corso di studi Laurea Magistrale

Sede Lecce

Crediti 6.0

Periodo Secondo Semestre

Ripartizione oraria Ore Attività frontale: 54.0

Tipo esame Orale

Per immatricolati nel 2024/2025

Valutazione Voto Finale

Erogato nel 2024/2025

Orario dell'insegnamento

<https://easyroom.unisalento.it/Orario>

### BREVE DESCRIZIONE DEL CORSO

Introduction to Computer Security  
Vulnerabilities of Set-UID programs  
Attacks based on Environment Variables  
Buffer Overflow attacks  
Introduction to Cryptography  
One-Way Hash Functions  
Secret-Key Encryption  
Public Key Cryptography  
Public Key Infrastructure  
Web security  
Transport Layer Security  
Bitcoin and Blockchain

### PREREQUISITI

Knowledge of the content of the course "System and Network Programming" ("Programmazione di Sistema") by the same teacher

### OBIETTIVI FORMATIVI

The course aims at providing the students with the basics of Computer Security. The course is based on UNIX®, the system which runs 86% of all publicly accessible servers (src: [https://w3techs.com/technologies/overview/operating\\_system](https://w3techs.com/technologies/overview/operating_system))

### METODI DIDATTICI

The course is strongly oriented towards a hands-on methodology.

### MODALITA' D'ESAME

Writing a program aimed at solving a given problem in a given time.

### ALTRE INFORMAZIONI UTILI

Computer Science is a very structured subject. Beware: missing a lecture could hinder understanding of all it follows.

---

## PROGRAMMA ESTESO

Introduction to Computer Security  
Vulnerabilities of Set-UID programs  
Attacks based on Environment Variables  
Buffer Overflow attacks  
Introduction to Cryptography  
One-Way Hash Functions  
Secret-Key Encryption  
Public Key Cryptography  
Public Key Infrastructure  
Web security  
Transport Layer Security  
Bitcoin and Blockchain

---

## TESTI DI RIFERIMENTO

Textbook:  
Wenliang Du. Internet Security: A Hands-on Approach, May 2022, ISBN 978-1733003964  
Wenliang Du. Computer Security: A Hands-on Approach, May 2022, ISBN 978-1733003957  
Additional, useful references:  
F. Tommasi "Alla Scoperta di UNIX - Esplorare GNU/Linux e macOS con la linea di comando" 2a edizione, Aprile 2024, ISBN: 979-1221056372