UNIVERSITÀ DI PISA

# FOUNDATIONS OF CYBERSECURITY

## GIANLUCA DINI

| | |
|---|---|
| Anno accademico | 2022/23 |
| CdS | COMPUTER ENGINEERING |
| Codice | 880II |
| CFU | 9 |

| Moduli | Settore/i | Tipo | Ore | Docente/i |
|---|---|---|---|---|
| FOUNDATIONS OF CYBERSECURITY | ING-INF/05 | LEZIONI | 90 | GIANLUCA DINI |

### Obiettivi di apprendimento

*Conoscenze*
Lo studente acquisirà conoscenze sulla crittografia applicata, la codifica sicura e la sicurezza web. Il corso ha l'obiettivo di mettere uno studente in grado di progettare e realizzare un'applicazione distribuita sicura.

Più precisamente, lo studente acquisirà una conoscenza dettagliata delle principal primitive crittografiche (cifari, funzioni hash, firme digitali), delle loro proprietà in termini di sicurezza e prestazioni e del loro uso appropriato nella progettazione e costruzione di protocolli e sistemi. Lo studente riceverà anche nozioni di base sulla codifica sicura, sulla sicurezza web e sui relativi principali attacchi, tra cui buffer overflow e iniezione SQL.

*Modalità di verifica delle conoscenze*
La verifica delle conoscenze avverrà per mezzo di una prova scritta e di una prova orale in ogni sessione d'esame.

*Capacità*
Alla fine del corso,

- lo studente saprà progettare e realizzare protocolli ed applicazioni distribuite sicure utilizzando una libreria crittografica;
- lo studente sarà in grado di presentare in una relazione scritta i risultati delle attività progettuale e di sviluppo svolte;
- lo studente sarà in grado di concepire e realizzare semplici attacchi di critto-analisi

*Modalità di verifica delle capacità*
Le capacità saranno verificate come segue:

- durante le sessioni di laboratorio informatico saranno svolti piccoli progetti tesi al comprendere l'utilizzo di una o più libreria crittografica;
- durante le sessioni di laboratorio informatico saranno svolti esempi di semplici attacchi di crittoanalisi ad algoritmi e schemi crittografici;
- alla fine del corso, prima dell'esame, lo studente dovrà preparare e presentare il progetto e la realizzazione di un'applicazione distribuita sicura, corredato da una relazione scritta che riporti i risultati dell'attività di progetto e di sviluppo.

*Comportamenti*
Lo studente potrà acquisire e sviluppare sensibilità alle problematiche relative alla cybersecurity ed all'impatto che questa viene avere sul business delle aziende, sui servizi della pubblica amminsitrazione e sulla sicurezza e privacy dei cittadini. A questo scopo, durante il corso saranno presentati casi reali presi dalla cronaca.

*Modalità di verifica dei comportamenti*
Durante la discussione del progetto sarà richiesto allo studente di discutere l'impatto che le misure di sicurezza progettate hanno nel contesto applicativo considerato.

### Prerequisiti (conoscenze iniziali)

- Calcolo delle probabilità
- Teoria della complessità

- Linguaggi di programmazione
- Architettura del calcolatore
- Sistemi operativi
- Reti di calcolatori

## Indicazioni metodologiche

- Lezioni frontali con l'ausilio di slide in formato pdf scaricabili dalla piattaforma del corso.
- Esercitazioni si svolgono in in aula informatica. Le esercitazioni sono state progettate in modo tale che lo studente possa utilizare il proprio PC in modo tale da semplificare la logistica della fase di studio individuale.
- Durante le esercitazioni, il docente è coadiuvato da un codocente.
- Il materiale didattico è distribuito attraverso la piattaforma del corso.
- Il docente comunica con gli studenti per mezzo dell'email o attraverso i ricevimenti istituzionali.
- L'insegnamento è erogato in lingua Inglese.

## Programma (contenuti dell'insegnamento)

**Applied cryptography**
Symmetric Ciphers: one-time pad, stream-ciphers, and block-ciphers. The DES and AES ciphers. Encryption modes. Hash functions: message digest codes and message authentication code. Black box attacks: the birthday attack. Diffie-Hellman key establishment. Asymmetric ciphers: the RSA, ElGamal and Elliptic Curvces cryptosystems. Digital signatures, certificates, certification authorities, and public key infrastructures. The X.509v3 certificate format. Perfect forward security. Secure Pseudo-Random Generators. Side-channel attacks: timing attack; fault-injection attacks; power analysis. Case studies: IpSec: ESP and AH mode; Secure Socket Layer: Handshake and Record protocol; Kerberos: basic scheme; the Ticket Granting Service; delegation, forwarding and proxiable tickets; realms.
**Programming secure applications**
Basics of secure coding in C/C++. The OpenSSL cryptographic library. Threat modeling: how to identify and prioritize vulnerabilities. Design and analysis of secure protocols. The BAN logic. Basics of web security: SQL injection and cross-site scripting.

## Bibliografia e materiale didattico

- Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners, Springer 2010
- Bruce Schneier. Applied Cryptography: : Protocols, Algorithms and Source Code in C. Wiley 2015
- Matt Bishop. Computer Security: Art and Science, 2nd edition. Addison-Wesley, 2019
- Materiale fornito dal docente.

## Indicazioni per non frequentanti

Nessuna

## Modalità d'esame

- L'esame è composto dalla discussione di un progetto, una prova scritta ed una prova orale.
- Il progetto può essere svolto da gruppi di massimo tre studenti. La discussione del progetto deve avvenire prima della sessione d'esame a cui lo studente vuole partecipare. Per discutere il progetto, gli studenti devono fissare tramite email un ricevimento con i docenti. Uno studente può partecipare ad una sessione d'esame solo se ha preventivamente sostenuto con successo la discussione del progetto. Se superata, la discussione del progetto rimane valida anche per gli appelli successivi.
- La prova scritta consiste in una o più domande ed uno o più problemi da risolvere. La prova scritta si svolge in aula e, se superata, rimane valida per un solo appello.
- La prova orale consiste in un colloquio tra il candidato e il docente, o anche tra il candidato e altri collaboratori del docente titolare.

**Durante la Fase 2**:

- La prova scritta è sostituita da un test di ammissione da svolgere online. Il test potrà prevedere domande con risposte a scelta multiple ovvero domande con risposte aperte. Il test si svolgerà sulla piattaforma Microsoft Team.
- La prova orale sarà svolta in modalità a distanza sulla piattaforma Microsoft Team.

Per quanto riguarda il test e la prova orale, la stanza virtuale è pubblicata sulla scheda di registrazione all'esame.
Nel caso di risposte aperte, il candidato deve scrivere su un foglio di carta, scattare una foto dell'elaborato e caricare il file grafico/pdf risultante sulla piattaforma Teams Una soluzione alternativa può essere l'utilizzo di un tablet o tavoletta grafica unitamente ad applicazioni grafiche come Microsoft Whiteboard (o equivalenti). Il file grafico/pdf risultante può essere inviato per per email ma solo come soluzione di emergenza preventivamente concordata con il docente.
Per quanto riguarda la prova orale, il candidato deve

1. dotarsi di uno o più fogli bianchi;
2. dotarsi di un pennarello nero o comunque di inchiostro scuro;
3. per tutta la durata della prova orale, inquadrare solo ed esclusivamente il foglio per mezzo di una telecamera (quella del PC o del cellulare).

Soluzioni alternative al foglio ed il pennarello possono essere:

1. tablet o tavoletta grafica (soluzione preferita in assoluto);
2. lavagna da inquadrare per mezzo di una telecamera.

Nel caso di utilizzo dello smartphone per l'inquadramento del foglio o della lavagna, il dispositivo deve essere fissato in una posizione stabile.

## Altri riferimenti web

Home page del Corso di Laurea Magistrale in Computer Engineering:
https://computer.ing.unipi.it/ce-lm
Home page dell'Università di Pisa
https://www.unipi.it/

## Note

Nessuna.

*Ultimo aggiornamento 19/09/2022 12:06*