Insegnamento di: Crittografia

Classe di laurea: LM66		**Corso di Laurea in:** Sicurezza Informatica	**Anno accademico:** 2020/2021
Denominazione inglese insegnamento: Cryptography		**Tipo di insegnamento:** Obbligatorio	**Anno:** I **Semestre:** I
Tipo attività formativa: Affine	**Ambito disciplinare:** Informatica	**Settore scientifico-disciplinare:** INF/01	**CFU totali:** 6 di cui CFU lezioni: 4 CFU ese/lab/tutor: 2

Modalità di erogazione, ore di didattica assistita ed ore dedicate allo studio individuale

ore di lezione: 32 ore di esercitazione/laboratorio/tutorato: 30

totale ore didattica assistita: 62

totale ore di studio individuale:

- 68 corrispondenti alle lezioni teoriche
- 20 corrispondenti alle esercitazioni guidate

Lingua di erogazione: Italiano	**Obbligo di frequenza:** no		
Docente: Costantina Caruso	**Tel:** 0805442305 **e-mail:** costantina.caruso@uniba.it	**Ricevimento studenti:** Causa emergenza sanitaria, il ricevimento studenti avviene esclusivamente in modalità digitale	**Giorni e ore ricevimento:** in qualsiasi momento via teams dal lun al ven

Conoscenze preliminari:

Conoscenze di matematica discreta, algebra e programmazione, del linguaggio di programmazione C

Obiettivi formativi:

Conoscenze e competenze teoriche, metodologiche e applicative in crittografia

Risultati di apprendimento previsti

Conoscenza e capacità di comprensione:

Conoscenza e comprensione di principi, algoritmi e protocolli crittografici; conoscenza e comprensione degli utilizzi della crittografia.

Conoscenza e capacità di comprensione applicate:

Capacità di valutare il grado di sicurezza di algoritmi e protocolli informatici; capacità di valutare il grado di sicurezza di sistemi informatici che usano strumenti crittografici.

Autonomia di giudizio:

Lo studente sarà in grado di valutare la qualità della soluzione crittografica usata rispetto alla tipologia di utilizzo, al livello di protezione richiesta in base alla quantità di potenza computazionale a cui un potenziale avversario può avere accesso, e rispetto all'intervallo di tempo presunto di utilizzo del sistema

Abilità comunicative:

Lo studente acquisirà abilità comunicative e adeguata appropriatezza espressiva per un registro di comunicazione non tecnico, adatto anche ad interlocutori non esperti del settore.

Capacità di apprendere:

Lo studente avrà la capacità di seguire l'evoluzione tecnologica di algoritmi e protocolli crittografici e di adeguare autonomamente il proprio livello di preparazione.

Programma del corso

- Introduzione alla crittografia
- Tecniche di cifratura classiche
- Crittosistemi a pacchetto
- Crittosistemi a chiave simmetrica

- DES, AES
- Crittosistemi a flusso, RC4
- Crittosistemi a chiave asimmetrica, RSA
- Algoritmi di Diffie-Hellman e di Elgamal
- Curve ellittiche e Bitcoin
- Protocolli crittografici: marcatura temporale di un documento, firma cieca, denaro elettronico, firma digitale
- Funzioni hash, funzioni MAC
- Gestione e distribuzione delle chiavi, autenticazione, Needam-Schroeder e Kerberos

Metodi di insegnamento:
Lezioni frontali
Esercitazioni guidate

Supporti alla didattica:

Controllo dell'apprendimento e modalità d'esame:
L’esame consiste in una prova orale.

Testi di riferimento principali:

A.J. Menezes, P.C. van Oorschot, S.A. Vanstone; Handbook of Applied Cryptography; CRC Press

William Stalling; Cryptography and Network security - Principles and practice - Global Edition - Seventh edition; Pearson

Slide del corso