ALLEGATO C

UNIVERSITA' DEGLI STUDI DI BARI ALDO MORO ANNO ACCADEMICO 2019/2020

DIPARTIMENTO DI INFORMATICA

Programma dell'insegnamento di: CRITTOGRAFIA

Corso di Laurea Magistrale in **Sicurezza Informatica**

SSD insegnamento INF/01 - CFU 6 - ore lezione 62 ore lezioni teoriche 32 ore laboratorio 30

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

Contenuti del corso

- Introduzione alla crittografia
- Crittosistemi, a pacchetto e a flusso
- Crittosistemi a chiave privata
- Crittosistemi a chiave pubblica
- Firma digitale
- Funzioni Hash
- Introduzione ai protocolli crittografici
- Protocolli crittografici di base: scambio di chiavi, autenticazione, Needam-Schroeder, Kerberos, One Time Password, Secret Splitting, Marcatura temporale di un documento
- Protocolli crittografici avanzati: firma cieca, denaro elettronico, crittomonete
- Applicazioni della crittografia: public key infrastructure, PGP, blockchain,bitcoin, KDC

Bibliografia

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

Slide docente

Modalità espletamento prova di esame (scritto, orale, scritto e orale, altro..)
Orale

E-mail del docente e/o suoi collaboratori : caruso.costantina@gmail.com

Ricevimento studenti: il mercoledì dalle 13,30 alle 15,.00 presso sede corso a Taranto.

Bari, 1 settembre 2019

Firma