Nome insegnamento: **Teoria della crittografia**

Dipartimento:	DIIES
Corso di laurea:	in Ingegneria Informatica e dei Sistemi per leTLC
Classe:	LM-27
Tipo Attività formativa:	altre attività
Ambito disciplinare:	a scelta
Settore Scientifico-Disciplinare:	MAT/03
Numero di Crediti Formativi Universitari:	6
Propedeuticità obbligatoria:	nessuna
Anno di corso:	II
Semestre:	II
Ore di insegnamento:	48
Modalità di esame:	Prova scritta ed orale

TITOLARE DEL CORSO

Prof.ssa Vittoria Bonanzinga

Obiettivi formativi

Conoscenza delle nozioni di base dell'Algebra, della Teoria dei numeri e della Geometria che risultano fondamentali nello sviluppo di protocolli crittografici. Conoscenza degli strumenti e delle tecniche proprie dell'Algebra, della teoria dei numeri e della Geometria per lo studio di protocolli crittografici. Capacità di comprendere ed utilizzare strumenti matematici adeguati per la risoluzione di problemi di Crittografia. Capacità di comunicare le conoscenze acquisite attraverso un linguaggio tecnico-scientifico adeguato.

Programma dettagliato

- Richiami sui numeri interi e sui campi finiti, aritmetica modulare, funzione di Eulero, teorema cinese del resto. Struttura di Z/pZ. Teorema di Gauss: esistenza delle radici primitive.

- Primalità e fattorizzazione: conseguenze del Piccolo Teorema di Fermat, numeri pseudoprimi, alcuni test di primalità (Fermat, Miller-Rabin), metodo(p-1) di Pollard per la fattorizzazione. Cenni sulla complessità degli algoritmi.

- Sistemi crittografici simmetrici e crittografia a chiave pubblica: RSA. Crittosistema di Diffie ed Hellman. Il problema del logaritmo discreto.

- Curve ellittiche: equazione di Weierstrass, gruppo dei punti di una curva ellittica, curve

ellittiche su campi finiti. Crittosistemi basati sulle curve ellittiche: scambio di chiavi di Diffie-Hellmann, protocollo di ElGamal.

-Fattorizzazione con le curve ellittiche, test di primalità con le curve ellittiche.

Testi consigliati

1. N. Koblitz. A Course in Number Theory and Cryptography, seconda edizione, Springer, 1994.

2. A. Languasco, A. Zaccagnini. Introduzione alla Crittografia, Ulrico Hoepli Editore, Milano, 2004.