

MATEMATICA (LB04)

(Lecce - Università degli Studi - Università degli Studi)

Insegnamento SISTEMI DI CIFRATURA E CODIFICA

GenCod A000951

Docente titolare Alessandro MONTINARO

Insegnamento SISTEMI DI CIFRATURA E CODIFICA **Anno di corso** 3

Insegnamento in inglese ENCRYPTION AND ENCONDING SYSTEMS **Lingua**

Settore disciplinare MAT/03

Percorso PERCORSO COMUNE

Corso di studi di riferimento MATEMATICA

Tipo corso di studi Laurea

Sede Lecce - Università degli Studi

Crediti 6.0

Periodo Primo Semestre

Ripartizione oraria Ore Attività frontale: 42.0 **Tipo esame** Orale

Per immatricolati nel 2013/2014

Valutazione Voto Finale

Erogato nel 2015/2016

Orario dell'insegnamento

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

BREVE DESCRIZIONE DEL CORSO

ITALIAN

Il corso intende fornire un background di metodi e risultati della Matematica Discreta utilizzati per la sicurezza della comunicazione odierna.

ENGLISH

The course aims to provide a background of methods and results of the Discrete Mathematics within today communication security.

PREREQUISITI

ITALIAN

Aver sostenuto gli esami di Geometria I, II e di Algebra I, II.

ENGLISH

Having passed the examinations of Geometry I, II and of Algebra I, II.

OBIETTIVI FORMATIVI

ITALIAN

Conoscenze e comprensione. Acquisire un'ampia conoscenza dei principi e degli strumenti matematici su cui si fonda la sicurezza delle comunicazioni segrete.

Capacità di applicare conoscenze e comprensione. Saper utilizzare diverse aree della matematica, come la teoria dei numeri, la teoria dei gruppi e dei campi, la teoria delle curve ellittiche e il calcolo delle probabilità discrete per la costruzione dei cifrari in uso per la sicurezza delle comunicazioni. Essere capaci di stabilire i punti di forza e di debolezza circa la sicurezza e la efficienza computazionali di un sistema crittografico.

Autonomia di giudizio. Saper estrapolare e interpretare i dati ritenuti utili a determinare giudizi autonomi riguardanti sia problemi strettamente collegati alle tematiche sviluppate nel corso, sia problemi non necessariamente di ambito matematico ma collegate alla sicurezza delle comunicazioni.

Abilità comunicative. Saper comunicare problematiche e soluzioni inerenti ad argomenti di Crittografia a interlocutori specialisti e non specialisti.

Capacità di apprendimento. Essere consapevoli come diverse aree della matematica concorrano nella soluzione di problemi concreti, come, ad esempio, la mediazione tra sicurezza delle comunicazioni e l'efficienza computazionale dei sistemi crittografici. Essere in grado di comprendere autonomamente testi di livello avanzato ed articoli scientifici, anche a livello di ricerca.

ENGLISH

Knowledge and understanding. Acquire a broad knowledge of the principles and mathematical tools on which the security of secret communications is based.

Applying knowledge and understanding. Knowing how to use different areas of mathematics, such as Number Theory, Group Theory, Field Theory, Theory of Elliptic Curves and the calculation of discrete probabilities for ciphers' construction of ciphers within communications security. Being capable of establishing the strengths and weaknesses of the computational security and efficiency of a cryptographic system.

Making judgments. To be able to extrapolate and interpret the useful data in order to determine independent judgments concerning both problems closely related to the issues developed in the course, and problems not necessarily of mathematical scope but connected to the security of communications.

Communication. Knowing how to communicate problems and solutions related to cryptography topics to specialists and non-specialist interlocutors.

Lifelong learning skills. Be aware how different areas of mathematics compete in solving concrete problems, such as, for example, between security and computational efficiency of cryptographic systems. Being able to autonomously understand advanced level texts and scientific articles, even at the research level.

METODI DIDATTICI

ITALIAN

Lezioni frontali ed esercitazioni.

ENGLISH

Lectures and exercises.

Elementi di Teoria dei Numeri. Sistema completo di residui modulo un intero. Piccolo Teorema di Fermat. Teorema Cinese dei Resti. Funzione "Phi" di Eulero. Teorema di Eulero. Radici primitive n-esime dell'unità. Simbolo di Legendre. Somme Gaussiane. Legge di Reciprocità Quadratica. Simbolo di Jacobi. Pseudoprimi. Numeri di Carmichael e relativa caratterizzazione. Teorema di Alford, Granville, Pomerance (enunciato). Pseudoprimi di Eulero. Test di Primalità di Soloway-Strassen. Pseudoprimi forti. Test di Primalità di Miller-Rabin.

Crittografia. Fondamenti: sistemi crittografici a chiave privata (simmetrici) e crittosistemi a chiave pubblica (asimmetrici). Firma digitale e funzioni hash. Conversione delle unità di messaggio in chiaro in interi o in elementi di un campo di Galois finito. Sistemi crittografici affini. Crittosistema RSA. Metodi di attacco al crittosistema RSA. Firma digitale basata sul crittosistema RSA. Il problema del logaritmo discreto. Protocollo di Diffie-Hellmann per lo scambio delle chiavi. Crittosistemi di Massey-Omura e di El Gamal. Firma digitale basata sul logaritmo discreto. Metodo di Pohlig-Silver-Hellman per il calcolo dei logaritmi discreti.

Curve Ellittiche. Proprietà generali delle curve algebriche piane. Cubiche. Equazione di Weierstrass di una cubica. Algoritmo di Nagell (cenno). Curve Ellittiche a coefficienti in un campo finito. Gruppo associato ad una curva ellittica. Teorema di Hasse (cenno) sul numero di punti di una curva ellittica a coefficienti in un campo finito. Curve ellittiche modulari e relativa legge di gruppo.

Crittografia basata su curve ellittiche. Costruzione di una curva ellittica. Conversione delle unità di messaggio in chiaro in punti di una curva ellittica a coefficienti in un campo finito. Analogo del crittosistema RSA basato su curve ellittiche (Koyama-Maurer-Okamoto). Il problema del logaritmo discreto per il gruppo associato ad una curva ellittica. Analoghi dei crittosistemi di Diffie-Hellman, Massey-Omura ed El Gamal. Firma digitale basata su curve ellittiche. Test di Primalità di Goldwasser-Kilian. Numeri e primi di Mersenne. Test di primalità di Lucas-Lehmer e analogo basato sulle curve ellittiche (Test di Gross). Fattorizzazione di interi attraverso le curve ellittiche. Algoritmo di Lenstra.

ENGLISH

Basics of Number Theory. Complete set of residues modulo an integer. Fermat's Little Theorem. The Chinese Remainder Theorem. The Euler "Phi" function. The Euler's theorem. Primitive n-th roots of the unity. The Legendre Symbol. Gaussian Sums. The Law of Quadratic Reciprocity. The Jacobi Symbol. Pseudoprimes. Characterization of Carmichael numbers. The Alford, Granville, Pomerance theorem (statement). Euler Pseudoprimes. The Soloway-Strassen Primality Test. Strong pseudoprimes. The Miller-Rabin Primality Test.

Cryptography. Basics: Private-key Cryptosystems (symmetric) and Public-key cryptosystems (asymmetric). Signature and hash functions. Conversion of plain message units into integers or into Galois field elements. The Affine Cryptosystem. The RSA Cryptosystem. Methods of attack on the RSA cryptosystem. Digital signature based on the RSA cryptosystem. The Discrete Logarithm Problem. The Diffie-Hellmann protocol for key-exchange. The Massey-Omura and The El Gamal cipher. The Digital signature based on Discrete Logarithm Problem. The Pohlig-Silver-Hellman algorithm for computing discrete logarithms.

Elliptic Curves. Plane algebraic curves. Cubic. Weierstrass equation of a cubic. Nagell's algorithm (nod). Elliptic curves over a finite field. The Group law of an elliptic curve. The Hasse's theorem for an elliptic curve over a finite field. Elliptic curves modulo an integer and related group law.

Elliptic curves cryptosystems. Construction of an elliptic curve. Conversion of plain text message units to points of an elliptic coefficient curve over a finite field. Analog of the RSA cryptosystem based on elliptic curves (The Koyama-Maurer-Okamoto cryptosystem). The discrete logarithm problem for the elliptic curve group. The Analogs of the Diffie-Hellman, Massey-Omura and El Gamal cryptosystems. Digital signature based on elliptic curves. The Goldwasser-Kilian Primality Test. Mersenne numbers and primes. The Lucas-Lehmer primality test and its analogue based on elliptic curves (The Gross Test). Factoring integers by means of elliptic curves. The Lenstra's algorithm.

TESTI DI RIFERIMENTO

1. N. Koblitz, A course in Number Theory and Cryptography, Springer, 2nd edition, 1999.
2. L. C. Washington, Elliptic curves. Number Theory and Cryptography, Chapman & Hall/Crc Florida, 2nd edition (2003)
3. Dispense del corso (*Course Notes*).