MATEMATICA (LM39)

(Lecce - Università degli Studi)

Insegnamento CRITTOGRAFIA

GenCod A005487

Insegnamento CRITTOGRAFIA

Anno di corso 2

Insegnamento in inglese CRITTOGRAPHY

Lingua ITALIANO

Settore disciplinare MAT/03

Percorso APPLICATIVO

Corso di studi di riferimento MATEMATICA

Docente Alessandro MONTINARO

Tipo corso di studi Laurea Magistrale

Sede Lecce

Crediti 9.0

Periodo Primo Semestre

Ripartizione oraria Ore Attività frontale: 63.0

Tipo esame Orale

Per immatricolati nel 2018/2019

Valutazione Voto Finale

Erogato nel 2019/2020

Orario dell'insegnamento https://easyroom.unisalento.it/Orario

BREVE DESCRIZIONE DEL CORSO

ITALIAN

Il corso è dedicato l'acquisizione dei principi della Crittografia Classica e Moderna. Particolare attenzione è dedicata alle tecniche matematiche utilizzate in ambito crittografico.

ENGLISH

The course is dedicated to the acquisition of the principles of Classical and Modern Cryptography. Particular attention is devoted to the mathematical techniques applied to Cryptography.

PREREQUISITI

ITALIAN

Aver superato Geometria I e II, Algebra I e II. Si richiede, inoltre, la conoscenza della Teoria delle Probabilità discrete ed elementi di Teoria della complessità computazionale.

ENGLISH

In order to attend the course, it s required to having passed Geometry I and II, Algebra I and II. The knowledge of Theory of Discrete Probability and basics of Theory of computational complexity is also necessary.

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.

MODALITA' D'ESAME

ITALIAN

L'esame finale consiste di una prova orale la cui durata è di circa 45' e consiste di almeno tre domande inerenti a parti del corso diverse. La prova è volta ad accertare le conoscenze acquisite nel corso e la capacità di esporle in maniera rigorosa. Lo studente supera l'esame se consegue un voto maggiore o uguale a 18/30.

Gli studenti italiani dovranno prenotarsi per sostenere l'esame finale utilizzando esclusivamente le modalità online previste dal sistema VOL.

Gli studenti ERASMUS dovranno effettuare la prenotazione dell'esame via mail all'indirizzo: *alessandro.montinaro@unisalento.it* almeno un giorno prima della data dell'esame. Nel caso di superamento della prova, la verbalizzazione del voto sarà effettuata mediante un verbale cartaceo.

ENGLISH

The final exam consists of an oral test which lasts about 45 minutes and consists of at least three questions concerning different parts of the course. The exam is aimed at ascertaining the knowledge acquired in the course and the ability to expose them in a rigorous manner.

The student passes the exam if he/she obtains a grade greater than or equal to 18/30. Italian students must register to take the final exam using only the online methods provided by the VOL system.

ERASMUS students must register the exam via email at: alessandro.montinaro@unisalento.it at least one day before the exam date. In the case of passing the exam, the grade will be recorded using an appropriate written report.

APPELLI D'ESAME

Calendario Appelli d'Esame a.a. 2019/2020

Sessione InvernaleSessione EstivaSessione AutunnaleSessione StraordinariaAppelli per Studenti Fuori Corso

10/01/2020

10/02/2020

24/02/2020

24/06/2020

23/07/2020

21/09/202008/01/2021

ALTRE INFORMAZIONI UTILI

PROGRAMMA ESTESO

ITALIAN

Crittografia classica. Fondamenti. Cifrario di Cesare, cifrario mediante sostituzione, cifrario affine, cifrario di Vigenère, cifrario di Hill, cifrario mediante permutazione. Crittosistemi a flusso. Principi della crittanalisi. Crittanalisi del cifrario affine, del cifrario mediante sostituzione, del cifrario di Hill. Crittanalisi dei cifrari a flusso LFSR. Elementi della Teoria di Shannon. Segretezza perfetta. Caratterizzazione dei cifrari perfetti. Cifrario One-time Pad. Cifrari prodotto.

Cifrari a blocco. Advanced Encryption Standard. Reti di sostituzione-permutazione (SPN). Crittanalisi lineare. Lemma Piling up. Approssimazione degli S-box. Attacco lineare alle SPN. Crittanalisi differenziale. Data Encryption Standard: descrizione ed analisi. Advanced Encryption Standard: descrizione ed analisi.

Funzioni Hash Crittografiche. Funzioni hash e integrità dei dati. Sicurezza delle funzioni hash. Il modello dell'oracolo random: algoritmi e confronto tra i sistemi di sicurezza. Funzioni hash iterate. La costruzione di Merkle-Damgård. L'algoritmo hash sicuro (SHA-1). Codici di autenticazione dei messaggi (MAC). MAC nidificati, HMAC, CBC-MAC. MAC incondizionatamente sicuri. Famiglie hash fortemente universali. Ottimalità della probabilità di inganno.

Il Crittosistema RSA e la fattorizzazione degli interi. Introduzione alla crittografia a chiave pubblica. Il crittosistema RSA. Test di Primalità: Soloway-Strassen, Miller-Rabin. Radici quadrate modulo un intero. Algoritmi per la fattorizzazione: algoritmo di p-1 di Pollard, algorithmo rho di Pollard, algoritmo di Dixon sui quadrati casuali. Ulteriori attacchi al RSA: calcolo della funzione di Eulero, esponente di decifratura, attaco di Wiener all'esponente basso di decifratura.

Crittosistemi a chiave pubblica basati sul Problema del Logaritmo Discreto. Crittosistema di El-Gamal. Algoritmi per il calcolo del problema del logaritmo discreto: algoritmo di Shank, algorithmo rho di Pollard per il problema del logaritmo discreto, Algoritmo di Pohlig-Hellmann. Curve ellittiche sui reali e sui campi finiti. Punti di compressione e sistemi di cifratura basati su curve ellittiche. Calcolo dei punti multipli su curve ellittiche. Sicurezza dei crittosistemi di El-Gamal. Crittosistema di Diffie-Hellmann.

Firma digitale. Requisiti di sicurezza per una firma digitale. Firma digitale e funzioni hash. Schema di firma digitale di El-Gamal e relative varianti. Schema di firma di Schnorr. Algoritmo di firma digitale. schema di firma basato s curve ellittiche. Schemi di firma dimostrabilmente sicuri. Firme digitali one-time. Full domain hash. Firme digitali non ripudiabili. Firme Fail-stop.

ENGLISH

Classical Cryptography. Basics. The Ceasar Cipher, the Substitution Cipher, the Affine Cipher, the Vigenère Cipher, the Hill Cipher, the Permutation Cipher. Stream Ciphers. Basics of Cryptanalysis. Cryptanalysis of the Affine Cipher, Cryptanalysis of the Substitution Cipher, Cryptanalysis of the Vigenère Cipher, Cryptanalysis of the Hill Cipher, Cryptanalysis of LFSR Stream Ciphers. Basics of Shannon's Theory. Perfect Screcy. Characterization of Perfect Ciphers. One-time Pad Chipher. Product ciphers.

Block Cihpers. Advanced Encryption Standard. Substitution Permutation Network (SPN). Linear Cryptanalysis. Piling up lemma . Approximation of S-boxes. A Linear attack on SPN. Differential Cryptanalysis. Data Encryption Standard: description and analysis. Advanced Encryption Standard: description and analysis.

Cryptographic Hash Functions. Hash functions and data integrity. Security of hash functions. The random oracle model: algorithms and comparison of security criteria. Iterated hash functions. The Merkle-Damgård construction. The secure hash algorithm (SHA-1). Message authentication codes (MAC). Nested MAC, HMAC, CBC-MAC. Unconditionally secure MAC. Strongly universal hash families. Optimality and deception probabilities.

The RSA Cryptosystem and factoring integers. Introduction to Public-Key cryptography. The RSA cryptosystem. Primality Tests: Soloway-Strassen, Miller-Rabin. Square roots modulo an integer. Factoring algorithms: the Pollard p-1 algorithm, the Pollard rho algorithm, Dixon's random squares algorithm. Other attacks on RSA: computing the Euler function, the decryption exponent, the Wiener's low decryption exponent attack.

Public-key cryptosystems based on the Discrete Logarithm Problem. The El-Gamal Crittosystem. Algorithms for the discrete logarithm problem: the Shank's algorithm, the Pollard rho discrete logarithm problem, The Pohlig-Hellmann algorithm. Elliptic curves over the reals and over finite fields. The poin compression and the Elliptic Curves Integrated Encryption Schemes. Computing multiple points on elliptic curves. Security of the El-Gamal cryptosystems. The Diffie-Hellmann Cryptosystem.

Signature Schemes. Security requirements for signature schemes. Signature and hash functions. The El-Gamal signature scheme and variants of it. The Schnorr signature scheme. The Digital signature algorithm. The elliptic curves DSA. Provably secure signature schemes. One-time signatures. Full domain hash. Undeniable signatures. Fail-stop signatures.

TESTI DI RIFERIMENTO

- O. Goldreich, Foundations of Cryptography, Cambridge University Press, 2001.
- J. Katz, Y. Lindell, Introduction to Modern Cryptography, Second Edition, Chapman & Hall/CRC, 2014
- N. Koblitz, A course in Number Theory and Cryptography, Springer, 2nd edition, 1999.
- D. R. Stinson, Cryptography Theory and Practice, Third Edition, Chapman & Hall/CRC 2005
- L. C. Washington, Elliptic curves. Number Theory and Cryptography, Chapman & Hall/Crc Florida, 2nd edition (2003)
- Dispense del corso- Course notes.