Università degli Studi di Roma "Tor Vergata"

Scheda Insegnamento

Mod. Scheda Insegnamento v. 1.1

Docente responsabile dell'insegnamento/attività formativa

Nome	Giulio
Cognome	Codogni

Denominazione insegnamento/attività formativa

Italiano	Crittografia
Inglese	Cryptography

Informazioni insegnamento/attività formativa

A.A.	2024/2025
	◉ L ○ LM ○ LM CU
CdS	Laurea Triennale in Matematica
Codice	8066111
Canale	
CFU	6
Lingua	Italiano

Docente del modulo didattico (compilare solo per attività formative articolate in moduli)

Nome	
Cognome	

Denominazione modulo didattico (compilare solo per attività formative articolate in moduli)

Italiano	
Inglese	

Università degli Studi di Roma "Tor Vergata"

Scheda Insegnamento

Obiettivi formativi e risultati di apprendimento attesi

Italiano	OBIETTIVI FORMATIVI: Capire come problemi matematici computazionalmente difficili possono garantire la sicurezza dei protocolli crittografici. Approfondire lo sudio dell'Algebra. CONOSCENZA E CAPACITÀ DI COMPRENSIONE: Conoscenza principi di base della crittografia e degli algoritmi crittografici più diffusi. Capacità di comprendere varianti di algoritmi crittografici noti. Conoscena degli argomenti di Algebra rilevanti per la crittografia. CAPACITÀ DI APPLICARE CONOSCENZA E COMPRENSIONE: Capacità di analisi di algoritmi crittografici. Comprensione del ruolo della matematica pura nella costruzione di protocolli crittografici. AUTONOMIA DI GIUDIZIO:
Inglese	LEARNING OUTCOMES: Understand how computationally-hard mathematical problems can gurantees the security of cryptographic protocols. Study some advanced algebra. KNOWLEDGE AND UNDERSTANDING: Basic principles of cryptography, and common cryptographic algorithms. Understand variants of well-known algorithms. Understand concepts from algebra relevant for cryptography. APPLYING KNOWLEDGE AND UNDERSTANDING: Being able of analyse cryptographic algorithms. Understand the role of pure maths within cryptographic algorithms. MAKING JUDGEMENTS:

Prerequisiti

Italiano	Elementi di algebra lineare, teoria dei gruppi, degli anelli e dei campi visti nei primi corsi di algebra e geometria. Carenze specifiche possono essere recuperate all'interno del corso. Potrebbe essere utile un minimo di familiarità con la teoria della probabilità e con dei linguaggi di programmazione.
Inglese	Linear algebra, group, ring and field theory, as in the syllabus of first years algebra and geometry courses. Specific weakness can be addressed during the course. Some familiarity with probability theory and with programming language could be useful.

Programma

Italiano	Studieremo gli algoritmi più utilizzati in crittografia, in particolare: - algoritmi simmetrici, in particolare Advanced Encryption Standard (AES). - funzioni di hash - algoritmi asimettrici basati su RSA, logaritmo discreto su campi finiti e su curve ellittiche. Seguriemo principalmente il testo di Stinson e Paterson citato nella bibliografia. Se il tempo lo permette, approfondiremo alcuni dei segunti argomenti:
Inglese	We will study the mosto common cryptographic algorithms, such as: - symmetric cryptography algorithms, such as Advanced Encryption Standard (AES) - hash functions - asymettric algorithms, such as the ones based on RSA, discrete logarithms on finite fields and elliptic curves We will mainly follow the textbook by Stinson and Paterson quoted in the bibliography. If we will have time, we can cover in details some of the following topics:

Modalità di valutazione

- ☐ Prova scritta
- ☒ Prova orale
- ☒ Valutazione in itinere
- ☐ Valutazione di progetto
- ☐ Valutazione di tirocinio
- ☐ Prova pratica
- ☐ Prova di laboratorio

Descrizione delle modalità e dei criteri di verifica dell'apprendimento

Italiano	Agli studenti che frequentano il corso verrà chiesto di consegnare settimanalmente o bi-setimanlmente degli esercizi. Alcuni esercizi verranno svolti alla lavagna dagli studenti stessi. Alla fine del corso gli studenti prepareranno una presentazione su un argomento a concordato con il docenti. Per gli studenti non frequntanti l'esame sarà orale e verterà su tutto il programma svolto e gli esercizi assegnati. I criteri di valutazione saranno i seguenti:
Inglese	Students attending the course will be asked to sole an exercise sheet every one or two weeks. Some exercises will be solved at the blackboard by the students. At the end of the course, studens will give a presentation on a topic agreed upon with the lecturer. The exam for students not attending the course will be oral. It will cover all the syllabus as well as the exercise sheets. The exam score is given by a mark expressed in thirtieths. The exam will be assessed according to the following criteria. Not suitable: Important deficiencies and/or inaccuracy in knowledge and understanding of

Testi adottati

Italiano	D. R. Stinson, M. Paterson, Cryptography, Theory and Practice, 4th Edition, Chapman and Hall/CRC, 2018
Inglese	D. R. Stinson, M. Paterson, Cryptography, Theory and Practice, 4th Edition, Chapman and Hall/CRC, 2018

Bibliografia di riferimento

Italiano	* W.M. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo, Aritmetica, crittografia e codici,Collana:UNITEXT. * D. Hans, K. Helmut, Introduction to Crypotography, 3rd Edition, Springer, 2015 * A. Laniguasco, A. Zaccagnini Manuale di Crittografia , Hoepli, 2015. * S. Vaudenay, A classical introduction to cryptography , Springer, 2006 * L. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd Edition, Taylor &
Inglese	* W.M. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo, Aritmetica, crittografia e codici,Collana:UNITEXT. * D. Hans, K. Helmut, Introduction to Crypotography, 3rd Edition, Springer, 2015 * A. Laniguasco, A. Zaccagnini Manuale di Crittografia , Hoepli, 2015. * S. Vaudenay, A classical introduction to cryptography , Springer, 2006 * L. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd Edition, Taylor &

Modalità di svolgimento

- [x] Modalità in presenza
- [ ] Modalità a distanza

Descrizione della modalità di svolgimento e metodi didattici adottati

Italiano	Buona parte del corso consisterà di lezioni frontali. Alcune ore verranno invece dedicate allo svolgimento degli esercizi assegnati dal libro di testo, sarà richiesta una parteciapazione attiva da parte degli studenti. Ci sarà ampio spazio per una discussione collettiva degli argomenti trattati.
Inglese	Most of the course will consist of frontal lectures. Sometimes we will do flipped classes. Students will be asked to actively partecipate to the lecture; there will be room for open discussion.

Modalità di frequenza

- (●) Frequenza facoltativa
- ( ) Frequenza obbligatoria

Descrizione della modalità di frequenza

Italiano	La frequenza non è obbligatioria ma fortemente consigliata.
Inglese	Attendence is strongly enoguraged, but it is not compulsory.