UNIVERSITÀ DEGLI STUDI DI PALERMO

DEPARTMENT	Ingegneria
ACADEMIC YEAR	2019/2020
MASTER'S DEGREE (MSC)	COMPUTER ENGINEERING
SUBJECT	CRYPTOGRAPHY
TYPE OF EDUCATIONAL ACTIVITY	B
AMBIT	50369-Ingegneria informatica
CODE	20612
SCIENTIFIC SECTOR(S)	ING-INF/05
HEAD PROFESSOR(S)	LO RE GIUSEPPE Professore Ordinario Univ. di PALERMO
OTHER PROFESSOR(S)	
CREDITS	6
INDIVIDUAL STUDY (Hrs)	108
COURSE ACTIVITY (Hrs)	42
PROPAEDEUTICAL SUBJECTS	
MUTUALIZATION	
YEAR	1
TERM (SEMESTER)	1° semester
ATTENDANCE	Not mandatory
EVALUATION	Out of 30
TEACHER OFFICE HOURS	**LO RE GIUSEPPE** Tuesday 15:00 17:00

DOCENTE: Prof. GIUSEPPE LO RE

PREREQUISITES	Computer Networks and Operating Systems
LEARNING OUTCOMES	Conoscenza e capacita' di comprensione (knowledge and understanding): Lo studente, al termine del corso, avra' acquisito conoscenze e metodologie per affrontare problematiche legate agli algoritmi di cifratura adottati nei moderni sistemi di elaborazione delle informazioni. Lo studente sara' in grado di analizzare algoritmi di cifratura a chiave simmetrica e pubblica e gli algoritmi di generazione dei numeri casuali adottati nell'ambito della sicurezza dei sistemi di elaborazione delle informazioni. Conoscenza e capacita' di comprensione applicate (applying knowledge and understanding): Lo studente avra' acquisito conoscenze e metodologie per analizzare la validita' e la complessita' di diversi algoritmi di cifratura. Autonomia di giudizio (making judgements): Lo studente avra' acquisito una metodologia di analisi dei meccanismi alla base dei moderni algoritmi di crittografia, giudicando la loro adeguatezza nella progettazione di sistemi sicuri per l'elaborazione delle informazioni. Abilita' comunicative (communication skills): Lo studente sara' in grado di discutere con competenza e proprieta' di linguaggio problematiche complesse legate agli algoritmi di crittografia. Capacita' di apprendere (learning skills): Lo studente sara' in grado di affrontare con autonomia l'analisi di qualsiasi algoritmo di crittografia.
ASSESSMENT METHODS	Written (mid-term and final written tests) and oral examination. Assessment procedure for the Written Exam During the course, according to the course timetable, students can do a mid-term test. Such exam has to be completed with the final test that will take place at the end of the course and before the regular exams. The written examination (mid-term + final, or unique written examination) will seek to determine the possession of skills, abilities and skills required. It includes at least three questions that aim to verify knowledge and understanding in the topics of the course, and the ability to apply knowledge and understanding to new problems. In the written exam the theoretical comments of the numerical findings are appreciated. The assessment is expressed in thirtieth and admission to oral test is determined by a minimum score (15), in case of lower score the exam fails. Evaluation criteria for the oral examination The oral test consists of an interview aimed to check that you have the skills and knowledge disciplinary provided by the course; the evaluation is expressed in thirtieths. The solutions proposed in the written examination will be discussed during the oral exam. Here, some questions will be asked to the students in order to test their achievement of educational goals and their communication skills. Moreover, in order to evaluate the ability to make independent judgements, the students will be asked to propose suitable solutions for a specific application scenario. The final evaluation will take into account both the score of the written exam (50%) and that of the oral exam. Excellent 30-30 and praise, outstanding knowledge of the topics, excellent properties of language, good analytical ability, the student is able to apply knowledge to solve complex problems. He should solve complex problems that require a deep understanding of all the topics of the course and the ability to jointly use them. He should also be able to know how to find the information needed to solve the problem. Very Good 27-29, Good command of the main topics, full of language, the student is able to apply knowledge to solve problems proposed. Good 24-26 good understanding of the main topics, discrete properties of language, with some abilities to independently solve the proposed problems. Satisfactory 21-23, the student has sufficiently mastered the main teaching subjects but he/she has the knowledge, satisfactory property language, limited ability to independently apply the knowledge acquired. Sufficient 18-20, Minimum basic understanding of the major teaching and technical language issues, very little or no ability to independently apply the knowledge acquired. Insufficient, it does not have an acceptable knowledge of the contents of the topics covered in the teaching.
EDUCATIONAL OBJECTIVES	The course aims to provide the students with a basic knowledge of cryptography. The course analyses cryptography techniques, their applications in cyber security, and their main features.
TEACHING METHODS	Lectures and computer laboratories

SUGGESTED BIBLIOGRAPHY	William Stallings – Cryptography And Network Security, 7th Edition

SYLLABUS

Hrs	Frontal teaching
6	Introduction to Cryptography
6	Symmetric Cyphers - DES, AES
4	Pseudorandom number generation
6	Public-key cryptography and RSA
4	Number theory and finite fields
2	Elliptic curve cryptography

Hrs	Practice
6	Symmetric Cyphers - DES, AES
6	Public-key cryptography and RSA
4	Number theory and finite fields
6	Symmetric Cyphers and Public-key cryptography
2	Exercises on elliptic curve cryptography