UNIVERSITÀ DEGLI STUDI DI PALERMO

DEPARTMENT	Ingegneria
ACADEMIC YEAR	2023/2024
MASTER'S DEGREE (MSC)	ELECTRONICS AND TELECOMMUNICATIONS ENGINEERING (FULLY ONLINE)
SUBJECT	CYBERSECURITY
TYPE OF EDUCATIONAL ACTIVITY	C
AMBIT	20925-Attività formative affini o integrative
CODE	19220
SCIENTIFIC SECTOR(S)	ING-INF/03
HEAD PROFESSOR(S)	GALLO PIERLUIGI Professore Associato Univ. di PALERMO
OTHER PROFESSOR(S)	
CREDITS	6
INDIVIDUAL STUDY (Hrs)	108
COURSE ACTIVITY (Hrs)	42
PROPAEDEUTICAL SUBJECTS	
MUTUALIZATION	
YEAR	2
TERM (SEMESTER)	2° semester
ATTENDANCE	Not mandatory
EVALUATION	Out of 30
TEACHER OFFICE HOURS	**GALLO PIERLUIGI** Friday 15:00 17:00 Ufficio del docente

DOCENTE: Prof. PIERLUIGI GALLO

PREREQUISITES	Basic knowledge of computer networks and programming skills in Java or Python.
LEARNING OUTCOMES	Knowledge and understanding At the end of the course, students will know theoretical concepts related to cryptography, system security, and network security. Students will be able to use common mathematical tools and algorithms for security, privacy and confidentiality both during data storage and transmission, as well as tools and methodologies for key exchange and basic elements for crypto currencies. For all these aspects, students will be able to recognize main vulnerabilities, attacks, and countermeasures. Applied knowledge and abilities Lectures will be supported by lab activities and supervised tutorials. Students will learn to apply their knowledge autonomously during their project essay and will be stimulated to troubleshooting and problem-solving. Students will be able to apply their knowledge on design security systems and protocols, using cryptographic primitives and standardized operational modes. Students will also be able to evaluate vulnerabilities and apply countermeasures to reduce and the threats by applying the proposed methodologies and tools. Making judgments Students will be able to apply theory to face real problems taking the appropriate decisions to solve them. Tutorials will reinforce acquired knowledge and skills and permit self-assessment. Communication skills At the end of the course, students will be able to properly expose features, principles and technical aspects of the presented architectures, systems and protocols using appropriate technical language. They will be able to design and deploy application services and security policies as well as interact/cooperate with engineers, designers and manufacturers. Learning abilities Several teaching techniques will be used to stimulate students' learning abilities, especially during tutorials. These include project work, cooperative learning, and brainstorming. During several sessions, students will be encouraged to study the problem autonomously, before providing them with one of possible solutions
ASSESSMENT METHODS	Students will be evaluated using the following examinations: oral discussion, project assignment accompanied by a short essay, and discussion of a scientific paper. These heterogeneous evaluation tools provide better assessment and permit to check the achievement of goals. Knowledge, understanding and communication skills will be evaluated through the oral discussion. Learning abilities and applied knowledge will be evaluated through the design and development of case study project, accompanied by a short essay. Independent judgment and the capability to autonomously select study material will be evaluated through the discussion of a scientific paper. This paper has to be chosen by the student, regarding one of the course topics. The overall grade will be the average score of the three components indicated above. GRADES 30-30 and laude: Excellent. Full knowledge and understanding of concepts and methods of the discipline, excellent analytical skills even in solving original problems; excellent communication and learning skills. 27-29: Very good. Very good knowledge and understanding of concepts and methods of the discipline; very good communication skills; very good capability of concepts and methods applications. 24-26: Good. Good knowledge of main concepts and methods of the discipline; discrete communication skills; limited autonomy for applying concepts and methods for solving original problems. 21-23: Satisfying. Partial knowledge of main concepts and methods of the discipline; satisfying communication skills; scarce judgment autonomy. 18-20: Acceptable: Minimal knowledge of concepts and methods of the discipline; minimal communication skills; very poor or null judgment autonomy. Non acceptable: Insufficient knowledge and understanding of concepts and methods of the discipline.
EDUCATIONAL OBJECTIVES	The course proposes an introduction to cyber security, explaining system vulnerabilities, protocol vulnerabilities. Cryptographic primitives and standardized operational modes will be discussed, in order to use them in real applications. The course has the following goals, grouped by argument. The first learning goal regards the analysis and the comprehension of vulnerabilities for networks, protocols, hardware and software systems. This

	includes also attacks, their detection, and countermeasures. The second learning goal is related to the use of standardized cryptographic primitives for stream ciphers and block ciphers, message authentication codes, key exchange mechanisms and digital signatures. The last learning goal is to give students the capability to autonomously evaluate pros and cons of centralized and decentralized approaches, basic mechanisms that enable crypto currencies, such as the blockchain, and use them in heterogeneous application contexts.
TEACHING METHODS	This course is composed of lectures, theoretical tutorials, and lab activities. These three aspects cover most of the studied topics. All the topics will be tackled under three complementary aspects: theoretical contents, vulnerabilities, and countermeasures. Lectures permit to transfer knowledge to students, stimulating their curiosity and highlighting the key topics of the course. These complete the comprehension of the course arguments. Theoretical exercises aim at stimulating learning and problem-solving. Laboratory activities are run both singularly and in a team, stimulating the application of knowledge, improving critical thinking as well as communicative and cooperative skills. Students are always guided by the instructor, and theoretical references are intertwined with guided exercises.
SUGGESTED BIBLIOGRAPHY	- D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, Ver. 0.4 - Sep. 30, 2017 publicly available https://toc.cryptobook.us/book.pdf - Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. 1996. CRC Press ISBN: 0-8493-8523-7

SYLLABUS

Hrs	Frontal teaching
3	Introduction to Symmetric ciphers
3	PRG (pseudo-random generators) and their predictability
3	semantic security, block cipher, PRP
2	DES (data encryption standard)
2	Feistel's Networks and Luby-Rackoff Theorem
2	Advanced Encryption Standard (AES)
3	Block ciphers from PRG. GGM method.
2	Mode of operation and their vulnerabilities
2	Message integrity. MAC (Message Authentication Code)
2	Digital certificates
2	Digital signature
2	Secure Socket Layer (SSL) Transport Layer Security (TLS)
3	Public key cryptography
2	Key management (Diffie-Hellman)
1	Password, phishing, spoofing
1	Smart cards
2	Network and application vulnerabilities
2	Passive and active attacks
2	Advanced Persistent Threats
2	Identification, Autentication, acces control
1	One time passwords
2	firewall, IDS, and IPS
2	Distributed consensus
3	Blockchain
2	Incentives
1	Overview of advanced cryptographic approaches