ENTITY	UNIVERSITY OF PALERMO - POLYTECHNIC SCHOOL
ACADEMIC YEAR	2014/15
BACHELOR DEGREE	Telecommunications Engineering
COURSE NAME	**Services and security on the Internet**
TYPE OF ACTIVITY	Distinctive teaching
DISCIPLINE	Telecommunications Engineering
TEACHING ID	16978
DIVISION IN MODULES	No
NUMBER OF MODULES	1
SCIENTIFIC DISCIPLINARY SECTOR	ING-INF / 03
INSTRUCTOR	**Pierluigi GALLO** Assistant Professor University of Palermo pierluigi.gallo@unipa.it
European Credit Transfer System (ECTS) CREDITS	12
NUMBER OF HOURS FOR PERSONAL STUDY	180
NUMBER OF HOURS DEDICATED TO ASSISTED TEACHING ACTIVITIES	104
PREPARATORY COURSES	Computer networks
YEAR COURSE	II
LOCATION OF CONDUCT OF LECTURES	DEIM
TEACHING ORGANIZATION	During the course, **lectures** will stimulate knowledge and understanding while **theoretical tutorials** will promote the use of these skills while facing a real problem. Problem solving during **laboratory activities** will be partly carried out by grouping students in clusters, stimulating interactions, increasing self-assessment procedures, and improving communication skills.
ATTENDANCE	Optional
EVALUATION CRITERIA	Students will be evaluated using homogeneous criteria and the following tools: oral examination, presentation of a short essay associated to a design and development case study. Additionally, the student may discuss a scientific paper. Heterogeneous evaluation tools provide better assessment and check if expected results are obtained. **Knowledge and understanding** will be evaluated through the oral examination and the short essay. **Independent judgment and communication**

	skills will be evaluated through the discussion of a scientific paper. **Learning abilities and applied knowledge and understanding** will be stimulated using tutorial sessions and a design and development case study. Both tools permit students to obtain a precise self-assessment of their abilities.
EVALUATION	Grades are on a scale of 30.
PERIOD OF LECTURES	Second semester
TEACHING CALENDAR	Please, visit www.ingegneria.unipa.it
OFFICE HOURS	Please, send an e-mail to the course professor and schedule an appointment

EXPECTED OUTCOMES

Knowledge and understanding
During the course, students learn several kinds of application services on the Internet, their enabling technologies, methods of their usage, configuration and developing. Cryptographic concepts as well as principles and practice of network security on the Internet will be presented and tested, services will be offered on the move, VoIP services and related protocols, web, mail and data transfer. Among expected results, there is the ability to evaluate architectural solutions and multimedia services.The course provides common mathematical tools and algorithms for security, privacy and confidentiality. Students learn to use appropriate technical language and to apply the proposed methodologies and tools by their own.

Applied knowledge
Lectures will be supported by lab activities and supervised tutorials. Students will learn to apply their knowledge autonomously, and will be stimulated to troubleshooting and problem solving. The development of a case study and a related short essay on the topic is requested at the end of the course or before the exam.

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. 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 brain-storming. During several sessions students will be encouraged to study the problem autonomously, before providing them with one of possible solutions.

OBJECTIVES MODULE

The course is intended for students that hold a bachelor degree and aims to train them on architectures, protocols and tools for application services on the Internet. Theoretical and technological aspects are faced in order to realize working systems and test-beds.

HOURS	**LECTURES**
2	Security: attacks, services, mechanisms, models.
	Symmetric encryption
2	Substitution and transposition
2	Block cipher and the Data Encryption Standard (DES)
2	Overview about finite fields
2	Advanced Encryption Standard (AES)
2	Symmetric ciphers
	Public key cryptography
3	Introduction to number theory
3	RSA algorithm (Rivest, Shamir, Adleman)
3	Key management
3	Message Authentication Code (MAC)
	Hash algorithms
2	Message Digest Algorithm (MD5)
2	Secure Hash Algorithm (SHA)
	Digital Signature
2	Digital Signature Algorithm (DSA)
	Applications for network security (basics)
2	X.509
1	PGP
1	S / MIME
1	IPSec
1	Secure Socket Layer (SSL)
1	Transport Layer Security (TLS)
2	Calls on the OSI stack
5	IPv6: Addressing, package size and differences with IPv4
3	Usage scenarios in IPv6
4	The application protocols HTTP, FTP, Jabber
3	Proxies and content filtering
5	Architectures, protocols and devices for VoIP
4	SIP / SDP
5	Peer-to-peer
1	Certified mail
3	Video streaming
3	Issues related to real-time applications
2	Location and georeferencing
5	Network Programming
	EXERCISES
3	The Asterisk platform
2	Tools for packet sniffing (wireshark, live http, ...)
6	Java in network programming
2	Setup and configuration of a streaming server
	SEMINARS AND DEBATES GUIDED
9	Seminars and guided debate of research in the field with the participation of industry experts
RECOMMENDED BOOKS	[1] Course slides [2] William Stallings, "Cryptography and network security"