
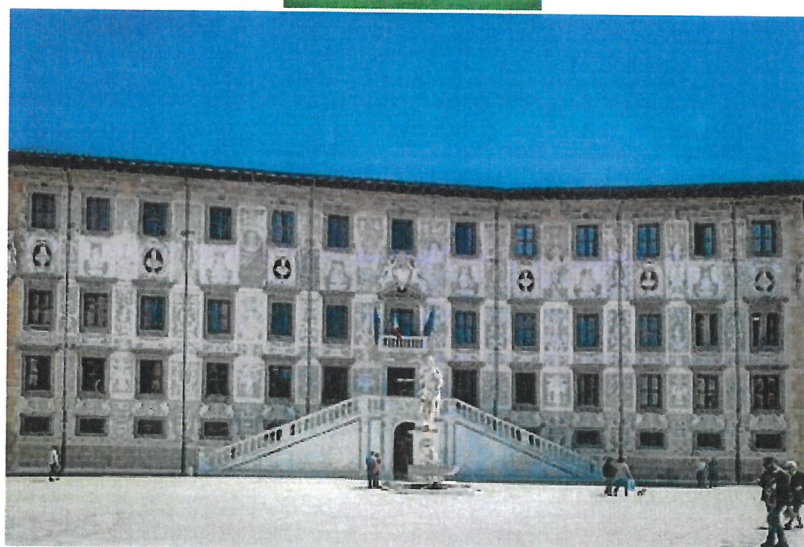
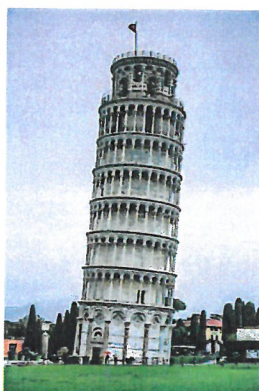




Fiche partenaire – Étudiants sortants (outgoing)

Universita di PISA	
Ville	PISA
Pays	ITALIE
Continent	Europe
Type de mobilité	Erasmus+
Cycle concerné	Master
Places disponibles	Master 1 et M2 : 4 places
Langues des cours	Anglais en cycle MASTER
Exigence linguistique	Basic italien recommandé – Anglais B1+
Autres exigences	Critère dossier scolaire.
Pourquoi cette université?	Fondée en 1343 - ancien élève et professeur à l'Université Galileo GALILEI, Enrico FERMI (1938) 56 000 étudiants Classement Shanghai ARWU 3/8 en Italie QS world university ranking 367th – dont 151/200 Medicine and Engineering Proximité – en Toscane près de Florence
Programme	www.unipi.it/academic-programmes www.unipi.it/programmes-in-English Master of science : Information & Communication technologies, Computer Engineering, Computer Science, Embedded Computer Systems, Electronics and automation, Biotechnology/Bionics.
Calendrier scolaire	Automne Cours : De fin septembre à Février Examens : Janvier-Février Hiver Cours : De fin février à fin Mai Examens : Juin-juillet www.unipi.it/educationalsystem
Accueil	international@unipi.it
Logement	www.unipi.it/accommodation entre 250 et 350 € https://housinganywhere.com
Cours de langue	Oui Language Center : www.cli.unipi.it
Site internet	www.unipi.it www.unipi.it/erasmus-programme
Section échange	Carlotta Del Chiaro – Sara Andreucci international@ingUnipi.it erasmus.incoming@ing.unipi.it
Guide pratique	 International Student Guide.pdf
Assurances	Carte vitale européenne + Mutuelle étudiante extension Europe www.unipi.it/eu-student-enrolment
Immigration	CI en cours de validité – Inscription pour un séjour de plus de 3 mois - EHC (S1 certificate for stays longer than 3 months)
Coût de la vie à prévoir	Coût de la vie similaire à celui de Toulon
Frais de scolarité	Aucun (Erasmus)

Démarche d'inscription	Nomination par l'ISEN Sélection par U. Pisa - www.unipi.it/eu-student-enrolment
Date limite	Automne Nomination : Fin mars Dossier complet envoyé au partenaire 1 ^{er} mai Hiver Nomination 1 ^{er} octobre Dossier complet envoyé au partenaire 31 octobre
Contact @école partenaire	Institutional coordinator : Prof. Francesco Marcelloni – international@unipi.it Responsible for incoming students : Ms Susanna Bianchi – erasmus.incoming@unipi.it Dpt of Information Engineering - Prof. Giuseppe Anastasi – giuseppe.anastasi@unipi.it School of Engineering website : http://www.ing.unipi.it/ Prof. Maria Greco – Coordinator Int. Relations : maria.greco@iet.unipi.it
Contact Isen	international-mediterranee@yncrea.fr



MsC in Cybersecurity – University of Pisa

The Master's Degree in Cybersecurity responds to the growing need for training of specialists with high scientific and technological expertise in the field of cybersecurity. To this end, it provides its graduates with a deep knowledge of the scientific foundations, methodologies and technologies of the area, which allows them to contribute to the advancement of knowledge and to be able to deal with cybersecurity in the most diverse application areas.

In particular, this is the first master's degree in Italy that addresses the security aspects at both hardware and software levels.

The degree also addresses the context of cybersecurity, consisting of organizations and companies that need to protect themselves from security risks, and the legal aspects of information security.

The degree program is designed to be profitably attended by students with strong knowledge of computer science or computer engineering from different degree classes, including those of Information Engineering classes and Computer Science and Technology.

The course is entirely delivered in English.

The master is offered by the departments of Information Engineering and of Computer Science of the University of Pisa.

Learnings Outcomes

- Knowledge of the scientific and technological aspects related to IT security and state-of-the-art solutions for the design, construction, verification and maintenance of safe and secure IT infrastructures and systems;
- knowledge of the aspects related to the organization of companies and the risk aspects related to the use of information technologies in the construction of their infrastructures and in data management;
- knowledge of the legal aspects regarding the protection of IT systems and treatment of data managed with digital tools; knowledge on how to design IT and data management systems in accordance with current legislation;
- ability to keep pace with technological innovation in cybersecurity, also by drawing on scientific publications in the field of cybersecurity
- ability to design and evaluate innovative IT security solutions

Career Opportunities

Designer of secure IT systems and applications

Design, development, evaluation, verification and management of complex communication systems and infrastructures to meet the most stringent security needs.

Skills: Deep knowledge of methodologies and technologies related to information security and of the legal aspects related to data processing and their security; ability to understand and integrate new technologies; strong capacity for critical analysis and evaluation of complex problems, also in relation to the many application areas in which the presence of secure IT systems is necessary; understanding of the company organization from the point of view of IT security.

Where: Companies, public bodies and public administrations operating in the field of production and IT services.

Cyber security researcher

Research and methodological and application innovation activities, in all areas of IT security.

Skills: deep knowledge of the scientific and technological foundations of IT security and secure data management; ability to abstract and to model complex IT systems and networks; knowledge of the problems posed by the interaction between IT security and other scientific / technological disciplines.

Where: public and private bodies operating in the IT security research sector, and scientific research in general. It is also possible to access subsequent university study levels, such as the PhD in Computer Science, Information Engineering and doctorates in related disciplines.

Cyber Security Specialist

Supervision, coordination and management of IT security policies and activities for companies and public administrations relating to the analysis, design, management and maintenance of information systems and networks.

Skills: the IT security specialist is skilled in technologies and methodologies for IT security and in the safe and reliable management of data. The specialist has also deep knowledge of the business organization and of the legal aspects of IT security, that allow him / her to cope with the various IT security needs of companies and public administrations. Specific skills concern the ability to analyze IT systems for the prevention, discovery, mitigation and recovery from cyber attacks, and the ability to design or remodel the existing IT infrastructures to meet specific security needs.

Where: Companies, public bodies and public administrations operating in the field of production and IT services.

Admission requirements and course structure

The degree program is free access.

The general curricular requirement for admission is the possession of a three-year degree in Computer Science (Class L-31), or in Information Technology (Class L-8).

Students with a 3-year Bachelor's degree from another class obtained in Italy or equivalent qualifications obtained abroad can be admitted if they have acquired at least 54 ECTS (Italian equivalent CFU) credits in the following sectors:

- At least 36 credits in ING-INF/01 (Electronics), ING-INF/03 (Telecommunication), ING-INF/05 (Computing Systems) sectors or INF/01 (Computer Science sector)
- At least 18 credits in the mathematics or physics sectors.

A good knowledge of English is required (Level B2 or higher).

Course structure

Year	First semester	CFU	Second semester	CFU
1	at choice – group A	12	Applied cryptography	9
1	Organizational sciences and information and technology law – module of Organizational sciences	6	Language-based technology for security	9
1	Data and system security	9	Organizational sciences and information and technology law – module of Information and technology law	6
1			Hardware and embedded security	9
Total		27		33
2	Secure software engineering	9	Dependability	6

2	Network security	9	Free choice 2	6
2	Free choice 1	6	Further activities	1
2	Artificial intelligence for security	6	Final MsC thesis defense	17
Total		30		30

Group A exams:

- Electronics and communication technologies – ECT (12 CFU)
- Systems and languages for informatics – SLI (12 CFU)

Electronics and communication technologies (ECT) is split in two modules:

- Electronics systems (6 CFU);
- Communication technologies (6 CFU);

Systems and languages for informatics (SLI) is split in two modules:

- Systems for informatics (6 CFU);
- Languages for informatics (6 CFU);

Free choice exams:

The following free choice exams at the second year are already activated:

- Electromagnetic Security (6 CFU)
- Penetration and defence laboratory (6 CFU)
- Biometrics systems (6 CFU)

Syllabus of the courses

Data and system security, 9 CFU

Overview: The course provides an up-to-date view of the latest developments of cybersecurity in data and system management, with the main reference to operating systems, distributed systems, and mobile systems. The covered topics are the definition of threats to computer systems and the discussion of the countermeasures that can be taken. For each covered topic, the course presents its foundations, the design aspects of secure systems and provides examples from the real world of standards and applications. Specific topics covered are:

- elements of computer security (threats, attacks, security requirements and defense strategies)
- elements of authentication and access control
- security in databases and datacenters
- attacks (malware, buffer overflow, denial of service,...)
- operative systems security (virtualization, case studies Linux, Windows, Android)
- security in mobile and cyber-physical systems
- aspects of management of computer security

Assessment method: Written and oral exam

Applied Cryptography, 9 CFU

Overview: The Applied Cryptography course provides an updated overview of the most recent developments in applied cryptography and its applications in the field of computer engineering for the design and implementation of products, protocols, services and secure systems. For each covered topic, the course presents the fundamental aspects in terms of security and performance properties. The course will make extensive use of examples taken from real world, standards and applications.

Topics include:

- Symmetric ciphers
- Asymmetric ciphers

- Secure hash functions: message digest codes and message authentication codes
- Secure random and pseudo-random bit generators
- Digital signatures, digital certificates, certification authorities
- Authentication and identification
- Key management
- Passwords
- Advanced cryptographic algorithms (blind signatures, Merkle tree, etc etc)
- Employment of cryptographic components in secure protocols, services and products by using the main programming languages
- Elements of cryptanalysis and side-channel attacks

Assessment method: Written and oral exam

Dependability, 6 CFU

Overview: The Dependability course provides the theoretical foundations of systems reliability and an updated overview of the methodologies for the design and development of safety-critical reliable applications, with reference also to cyber-security threats.

Topics include:

- Dependability attributes: Reliability, Availability, Safety, Confidentiality, Integrity, Maintainability.
- Definition of faults, errors and failures. A taxonomy of faults. Relation between Reliability and Security: malicious faults.
- Fault tolerance techniques: Hardware redundancy, Information redundancy and Software redundancy.
- Concepts of consistency, validity and agreement in distributed systems. Byzantine Agreement.
- Mathematical models of reliability: probability density function and failure rate. Exponential failure law of the hardware; models for reliability of software. Mathematical models of availability: repair rate.
- Reliability Block Diagrams, Fault trees/Attack trees, Markov chains.
- Hazard analysis and Risk analysis, in case of cyber-security threats.
- Standards for safety-critical systems, with reference to a specific context (e.g., automotive systems).

Assessment method: Written and oral exam

Artificial Intelligence for Cybersecurity, 6 CFU

Overview: The course aims to introduce the main methods and techniques of artificial intelligence used in information security applications. In particular, the course introduces topics such as data pre-processing, frequent pattern mining and association rules, classification, clustering, anomaly detection. In addition, the course discusses the main attacks against artificial intelligence systems, such as the adversarial classifier evasion and data poisoning, and the related defensive techniques. Finally, the course deals with the main uses of artificial intelligence in information security problems such as the detection of spam/phishing, the detection of intrusions and malware, the detection of online frauds, the analysis of the cyber threat intelligence.

Details of the topics covered:

- Data preprocessing
- Frequent pattern mining
- Classification
- Clustering
- Outlier detection
- Adversarial machine learning
- AI applications for spam and phishing detection
- AI applications for intrusion and malware detection
- AI applications for fraud detection
- Cyber threat intelligence analysis

Assessment method: Written and oral exam

Systems for informatics (6 CFU, module of Systems and Languages for Informatics)

Overview: This module is aimed at improving the preparation of students graduated in disciplines different from computer science/engineering in the field of computer systems and networks. The objective is to provide the basic elements about hardware architecture, operating systems, and computer networking as tools for implementing applications and services in the area of cybersecurity. Topics considered in the module include:

- Assembly language
- Interrupt mechanism
- User and System state
- Processes and Context Switch
- Memory management, virtual memory
- Input/Output
- File system
- Databases
- Computer Networks
- Distributed applications
- Wireless/Mobile Networks

Assessment method: Written and oral Exam

Languages for informatics (6 CFU, module of Systems and Languages for Informatics)

Overview: The Languages for Informatics module aims at improving the preparation of students graduated in disciplines different from computer science/engineering in the fields of computer programming, languages and algorithms. Specifically, it provides the basic elements of the constructs, functions and data structures of modern programming languages, it introduces the concepts of computational complexity and basic algorithms for typical problems and data structures. Topics considered in the module include:

- programming: basic constructs, functions and their mechanisms, data structures
- finite state automata
- introduction to computational problems
- complexity: models, input and output size, decision trees, lower and upper bounds, bad case and average case
- algorithms on sequences, dynamic programming, combinations and permutations, divide et impera
- trees, hash tables

Assessment method: written and oral exam

Electronics Systems (6 CFU, module of Electronics and Communication Technologies)

Overview: The main objective of the Electronics Systems course is to provide a common Electronics background to perspective students coming from different three years bachelor studies, in which the Electronics topics have been dealt with different views and different depths, and to let the students acquire a common and shared vocabulary on the Electronics Systems domain.

As far as the technical contents of the course are concerned, the students will acquire competences on and knowledge about the main electronic platforms used in cybersecurity applications

Main topics:

- How to make information digital: ADC and DAC description, with emphasis on the architectures, features and performance of the most common converters between the analog and digital domains. General recalls about logic networks and digital electronic circuits.
- Electronic Digital Signal Processing: platforms for realizations of functions programmable in software and hardware. Characteristics, performance, applicability scenarios as a function of the targeted application.
- Definition and performance comparison of the most common programmable architecture such as FPGA, PLA, PAL, DSP, GPU, FPSOC, ASIC.

- Characteristics and performance of an MCU platform (MicroController Unit). Computer peripherals aimed at cybersecurity applications.
- Hardware/Software co-design methodologies and Hardware Description Languages (HDL) for the hardware design of complex logic functions.
- HDL and design methodologies for digital designs on programmable logic (FPGA, FPGa) or custom hardware (CMOS standard cells and Intellectual Property cores).

Assessment method: Oral Exam

Hardware and embedded security, 9 CFU

Overview: The course Hardware and embedded security aims at providing the required skills to analyze, design and verify dedicated HW solutions or HW/SW embedded systems (e.g. Hardware security modules integrated in general purpose processors) for several cryptographic functions for encryption/decryption, signature and anomaly/intrusion detection. The course will also present application examples of HW security and embedded security to IoT, Automotive or Industry4.0 case studies.

More in details the course will cover the following subjects:

- High Level Synthesis & design of accelerators for cryptographic functions in embedded systems. HW/SW co-design for cybersecurity and comparison of SW-based solutions vs HW-based ones in terms of energy efficiency, real-time operating capability, flexibility, cost and size.
- Examples of HW accelerators for cybersecurity for asymmetric and symmetric cryptography and for signature (e.g. coprocessors for AES, SHA, ECC) and evolution towards post-quantum cryptography
- Embedded solutions for anomaly/intrusion detection
- Analysis of cryptographic accelerators embedded in General Purpose processors (e.g. HSM-Hardware Security Modules in Intel and/or ARM and/or Aurix platforms)
- Correlations among security and safety issues.
- Technologies and architectures for secure storage of data and keys and Smart cards
- Technology trends for on-chip generation of random data, Physically Unclonable Functions (PUF), HW Random Number Generation (e.g. TRNG/CSPNRG)
- Physical levels “side-channel” cybersecurity attacks (by analyzing thermal, power and electrical signals).
- Examples of application of HW security and embedded security to IoT, Automotive or Industry4.0 case studies

Assessment method: Oral Exam

Biometric systems, 6 CFU

Overview: This course provides fundamentals about techniques to verify or recognize the identity of a living person based on the analysis of biological/physiological traits and/or behavioural features.

In detail:

- Biometrics overview (history of biometrics, applications)
- Recognition, identification and verification
- Privacy, security and ethics
- Overview of image processing
- Physiological biometric systems: fingerprint recognition, face recognition, iris recognition, retina recognition, hand recognition, vein patterns
- Behavioral biometric systems: keystroke dynamics, signature recognition, voice recognition, gait recognition
- Multi-modal biometric systems
- Biometric applications

Exam modality: oral exam

Communication technologies (6 CFU, module of Electronics and Communication Technologies)

Overview: The aim of the Communication Technologies module is to provide the necessary background for those coming from three-year degree courses in which studies of digital communication systems and technologies have not already been addressed. The training objective is to provide knowledge of the architectural characteristics and basic technologies of the main communication systems for the transport and access network (also wireless), also presenting specific examples. The course will provide students with i) general knowledge of the basic technologies that allow the design of wired (copper, fiber) and wireless communication systems, ii) a specific knowledge of the main communication standards for transport and access networks, and iii) in-depth knowledge of robust spread spectrum transmission techniques.

Topics include:

- Basic concepts on digital signals, information theory and Shannon's theorem
- Digital modulation and wireless radio propagation models
- Generations of cellular networks (2G, 3G, 4G, 5G) and their multiplexing and multiple access technologies with particular attention to CDMA, OFDM and OFDMA
- Technologies for the access network on copper twisted pair, with particular reference to the xDSL family.
- Technologies for transmission on optical fiber in the transport network (optical backbones) and in the access network, with particular reference to the FTTx family
- Safe and robust communications through spread-spectrum technology: Direct-Sequence, Frequency-Hopping, Time-Hopping, and Chirp.

Assessment method: final oral exam

Network security, 9 CFU

Overview: The main goal of the Network Security course is to provide students with skills in security management technologies for wired and wireless networks. The training goals of the course are i) to provide the necessary knowledge on information security technologies most used in the Internet and corporate networks, ii) to provide the skills necessary for the design of secure networks and the evaluation of the security of existing networks, iii) to provide knowledge about specific security problems in wireless networks and iv) to make known the security mechanisms provided in the standards of WLAN networks and mobile systems. Topics include:

- Network access control: Extensible Authentication Protocol
- Intrusion Detection Systems and Firewalls
- IP layer security threats and IPSec protocol
- DNSSEC
- Transport layer security protocols: Transport Layer Security
- Security threats of Web services and HTTPS protocol
- Security threats of e.mail services and S/MIME
- Security issues in wireless networks: threats and countermeasures for improvising the wireless communication security
- WLAN security issues: the standard IEEE 802.11i
- Security threats in wireless mobile networks, the countermeasures defined in the 3GPP standards: procedures and protocols for securing GSM/GPRS, UMTS, LTE and 5G systems.

Assessment method: oral exam

Electromagnetic Security, 6 CFU

Overview:

The main objective of the course is to introduce the problem of security issues due to intentional and unintentional electromagnetic signals as well as countermeasure methods.

Specifically, students will acquire the following competences: i. how an information and communication system is vulnerable to radiated and conducted electromagnetic fields; ii. how to design electromagnetic shielding and secure rooms for data protection from electromagnetic threats; iii. which NATO standards and procedures are currently in use for limiting the information leakage through radiated and conducted electromagnetic signals.

Main topics

- Electromagnetic threats - Vulnerability of information systems to electromagnetic threats
- Undesired emissions from non-intentional sources and E.M. signals interception: E.M. propagation fundamentals
- Spectrum sensing and monitoring - Radiogonometry systems - Signal demodulations - Omnidirectional and directional antennas
- E.M. Shielding and secure rooms: effect of materials, effect of apertures and cable connections. Coupling mechanisms of e.m. signals. Zoning of infrastructures.
- Active security and intentional interferences: Radio Jamming - Friendly jamming for secure wireless communications
- Standards and measurement procedures: COMSEC and TEMPEST (Transient Electromagnetic Pulse Emanation Standard) - National and international (NATO) standards - TEMPEST equipment and devices

Assessment method: oral

Penetration and defence laboratory, 6 CFU

Overview: The course will give hands-on experience on the most important techniques used in the exploitation of software and hardware vulnerabilities, and the countermeasures adopted to mitigate such attacks. Topics include:

- OS (unix/linux): suid/sgid binaries, environment variables, symlink attacks, sandboxing via containers and/or Virtual Machines;
- programming: stack and heap overflow, format string vulnerabilities, integer overflow, shellcodes and Return Oriented Programming, side-channels, NX, W^X, ASLR and PIE, binary reversing
- hardware: Rowhammer, Meltdown, Spectre and their mitigations
- network: network scanning, service scanning, fuzzing
- web applications: mapping, authentication vulnerabilities, login bruteforcing, session management vulnerabilities, session hijacking, SQL injection, LDAP injection, cross-site scripting

modalità di esame: progetto e prova orale

Language-based technology for security, 9 CFU

Overview - Traditionally, computer security has been largely enforced at the level of operating systems. However, operating-system security policies are low-level (such as access control policies, protecting particular files), while many attacks are high-level, or application-level (such as email worms that pass by access controls pretending to be executed on behalf of a mailer application). The key to defending against application-level attacks is application-level security. Because applications are typically specified and implemented in programming languages, this area is generally known as language-based security. A direct benefit of language-based security is the ability to naturally express security policies and enforcement mechanisms using the developed techniques of programming languages.

The aim of the course is to allow each student to develop a solid understanding of application level security, along with a more general familiarity with the range of research in the field. In-course discussion will highlight opportunities for cutting-edge research in each area. The course intends to provide a variety of powerful tools for addressing software security issues:

- To obtain a deeper understanding of programming language-based concepts for computer security.
- To understand the design and implementation of security mechanisms.
- To understand and move inside the research in the area of programming languages and security.

Content - This course combines practical and cutting-edge research material. For the practical part, the dual perspective of attack vs. protection is threaded through the lectures, laboratory assignments, and projects. For the cutting-edge research part, the course's particular emphasis is on the use of formal models of program behaviour for specifying and enforcing security properties.

Topics include:

- Certifying Compilers
- Code obfuscation
- In-lined Reference Monitors
- Formal Methods for security
- Security in web applications

- Information Flow Control

Lab assignment and final Assessment method - There are lab assignments. The lab assignments are experimental activities about specific problems. To pass the course, students must pass the labs by making a presentation of the assignments in class and pass the requirements on a written report that documents the activities done.

Learning Goals - After the course, students should be able to apply practical knowledge of security for modern programming languages. This includes the ability to identify application- and language-level security threats, design and argue for application- and language-level security policies, and design and argue for the security, clarity, usability, and efficiency of solutions, as well as implement such solutions in expressive programming languages. Student should be able to demonstrate the critical knowledge of principles behind such application-level attacks as race conditions, buffer overruns, and code injections. You should be able to master the principles behind such language-based protection mechanisms as static security analysis, program transformation, and reference monitoring.

Secure Software Engineering, 9 CFU

Overview: The aim of the course is to introduce security-aware, advanced software engineering techniques. The course includes a 3 ECTS hands-on lab for active learning, and continuous assessment activities during the term.

Topics include:

- Agile software development (Agile principles, user stories)
- Microservices (motivations, definition, properties, case studies)
- Security in application design (confidentiality, integrity, availability)
- Static analysis of software security (vulnerability analyses)
- Secure software deployment (cloud- and container-based)
- Dynamic analysis of software security (development/release/user testing, monitoring)
- Security in Edge and Fog computing

Assessment method: Continuous assessment and oral exam

Organizational sciences, 6 CFU

Overview: the course will provide students with basic organizational knowledge with particular regard to the topics of structure, strategy, organizational culture, interorganizational networks, knowledge management and organizational learning. Some knowledge of organizational behavior in terms of team building and leadership will also be provided.

The course will also provide knowledge about the tools and methodologies for the correct analysis and implementation of information systems in the organizational context. In particular, in-depth knowledge of the Information Technology tools that have the greatest impact on the performance and effectiveness of organizations, such as CRM or ERP systems, will be deepened. Particular attention will be paid to the phenomena of big data and organizational profiles of cybersecurity

Topics detail:

- Organizational responses for cybersecurity
- The organizational structures and their types
- The strategic process
- Organizational culture and related typologies
- Interorganizational networks,
- Knowledge management
- Organizational learning
- Organizational applications of Information Technology, such as systems of:
 - Intranet
 - Enterprise Resource Planning (ERP)
 - Customer Relationship Management (CRM)
 - Decision Supporting (DSS): Management Information, Executive Information
 - Big data and possible organizational structures

- Supply Chain Management

Assessment method: written and oral exam.

Information and technology law, 6 CFU

Overview: The course addresses the legal rules applicable to computer technologies and their implementation in cybersecurity systems. Specific attention will be devoted to the legal framework applicable at national and supranational level, and the standards of protection required by law as regards data protection, copyright and the liability regimes applicable. For each topic, the course will provide the legal framework the open issues that still emerge in the practical implementation, and the solutions provided by courts. Specific topics covered are:

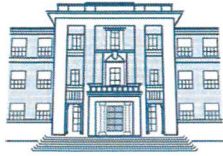
- Legal definition of cybersecurity at national and European level
- Data protection and data security – privacy by design and risk assessment
- Data protection and artificial intelligence
- Digital signatures, certification authorities and other authentication systems.
- Data breach e Liability regimes
- Intellectual property and copyright
- Blockchain technology and its legal aspects

Assessment method: Written and oral exam

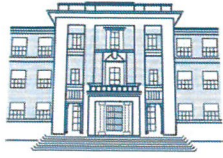


ENGINEERING-UNIPi-Fact Sheet-Erasmus+ 2023-2024

UNIVERSITY OF PISA	
Name	Università di Pisa
Erasmus University Code	I PISA 01
International Office (Central)	<i>Institutional Coordinator</i> Prof. Giovanni Federico Gronchi international@unipi.it <i>Responsible for incoming students</i> Ms Susanna Bianchi, erasmus.incoming@unipi.it
Website	https://www.unipi.it/ (Italian) https://www.unipi.it/index.php/english (English)
DEPARTMENTS OF THE ENGINEERING AREA	
Dipartimento di Ingegneria dell'Energia, dei Sistemi, del Territorio e delle Costruzioni (DESTEC)	<i>Director</i> Prof. Rocco Rizzo rocco.rizzo@unipi.it
Department of Energy, Systems, Territory and Constructions Engineering	<i>Coordinator for Intl. Relations (CAI)</i> Prof. Sauro Filippeschi sauro.filippeschi@unipi.it <i>Assistant to Coordinator for Intl. Relations</i> Ms. Marina Flaibani marina.flaubani@unipi.it <i>Website</i> https://www.destec.unipi.it/



<p>Dipartimento di Ingegneria Civile e Industriale (DICI)</p> <p>Department of Civil and Industrial Engineering</p>	<p><i>Director</i> Prof. Maria Vittoria Salvetti maria.vittoria.salvetti@unipi.it</p> <p><i>Coordinator for Intl. Relations (CAI)</i> Prof. Paolo Sebastiano Valvo paolo.sebastiano.valvo@unipi.it</p> <p><i>Assistant to Coordinator for Intl. Relations</i> Ms. Alessia Bartalucci alessia.bartalucci@unipi.it</p> <p><i>Website</i> https://dici.unipi.it/</p>	
<p>Dipartimento di Ingegneria dell'Informazione (DII)</p> <p>Department of Information Engineering</p>	<p><i>Director</i> Prof. Andrea Caiti andrea.caiti@unipi.it</p> <p><i>Coordinator for Intl. Relations (CAI)</i> Prof. Luca Sanguinetti luca.sanguinetti@unipi.it</p> <p><i>Assistant to Coordinator for Intl. Relations</i> Ms. Sara Andrenucci sara.andrenucci@unipi.it</p> <p><i>Website</i> https://www.dii.unipi.it/</p>	
INTERNATIONAL EXCHANGE AGREEMENTS/NOMINATIONS - Contacts		
Bilateral Agreements	Marina Flaibani (DESTEC) Alessia Bartalucci (DICI) Sara Andrenucci (DII)	international@ing.unipi.it
Incoming Students - Nominations and applications	Marina Flaibani (DESTEC) Alessia Bartalucci (DICI) Sara Andrenucci (DII)	erasmus.incoming@ing.unipi.it



NOMINATION AND APPLICATION PROCEDURE

TO BE DONE BY PARTNER UNIVERSITIES

Nomination procedure for Erasmus+ mobility	<p>e-mail message including: Student Personal Info (Name, Surname, birth date, Nationality) Agreement ISCED area Department of Interest Number of months</p> <p>Deadlines: First semester/Full Academic year: July 15th Second Semester: December 15th To: erasmus.incoming@ing.unipi.it</p>
---	---

TO BE DONE BY NOMINATED STUDENTS

Application procedure for nominated students Info: http://www.ing.unipi.it/en/international/incoming-mobility/erasmus-incoming	Compulsory Documents to be submitted: Learning Agreement (2023-2024 version) Courses Unit List Language certificate (Italian B1 and/or English B2) <i>Documents should be signed both by the student and the Home Institution</i> To: erasmus.incoming@ing.unipi.it
Enrolment at UNIPI Info: http://www.ing.unipi.it/en/international/incoming-mobility/erasmus-incoming	Registration on Alice Portal Submission of the Application Form on UNIPI's website Further information on how to finalize your application at UNIPI will be notified later.

PRACTICAL INFORMATION

International Support	Students	Central International Office Contacts https://www.unipi.it/index.php/welcome-and-support/itemlist/category/305
Accommodation		international@unipi.it https://www.unipi.it/index.php/student-services/item/2322
Visa and Residence Permit		international@unipi.it https://www.unipi.it/index.php/welcome-and-support

ACADEMIC INFORMATION



Academic Calendar	http://www.ing.unipi.it/en/study/academic-calendar
Language Requirements	Compulsory level of Italian B1 (for courses offered in Italian) / English B2 (for courses offered in English) - a language certificate or a statement from the Home University confirming the level of knowledge is mandatory.
Italian Language Courses	Courses in Italian language are offered by the Centro Linguistico https://www.cli.unipi.it/area-internazionale?set_language=en&cl=en
Programmes taught in English	https://www.unipi.it/index.php/study/itemlist/category/524
Courses Offer	Engineering courses for 2023-2024 available on-line in June A pdf list will be sent to nominated students For previous academic years: https://www.unipi.it/index.php/academic-programmes/itemlist/category/533
<p>Some general rules should be taken into account when choosing courses:</p> <ol style="list-style-type: none">1. Courses are offered by the Department and in the ISCED area and level covered by the agreement with the Home Institution;2. We allow students to include courses, with a certain degree of flexibility, from all our 3 Engineering Departments, but this is subject to assessment;3. It is also possible to include courses from other UNIPI Departments (max 6 ECTS/semester), but this is subject to approval by the relevant Erasmus Coordinators;4. If courses are chosen from different years of course and/or degrees it is highly probable that there will be overlapping of classes;5. Courses are offered in the semester covered by the mobility;6. Yearly courses (semester 1 and 2) might be split up into modules, but this is subject to approval by the teachers;7. It is possible to include one or more Italian language courses, for 4 ECTS credits each. Only the first course is free of charge;8. The possibility to include a final project in the LA is subject to confirmation of availability by a supervisor in Pisa;9. Our offer at undergraduate (BSc) level is totally taught in Italian language;10. Bachelor students can only choose courses offered at BSc level. In case of bachelor courses lasting more than 3 years, BSc students can access courses at MSc level if they have completed all the activities of their 3rd year.	