UNIVERSITA' DEGLI STUDI DI MILANO
PROGRAMME DESCRIPTION - ACADEMIC YEAR 2025/26
MASTER DEGREE
CYBERSECURITY (Classer LM-66 R)
Enrolled in 2025/26

HEADING

Degree classification - Denomination and code:	LM-66 R
Degree title:	Dottore Magistrale
Length of course:	2
Credits required for admission:	180
Total number of credits required to complete programme:	120
Years of course currently available:	1st
Access procedures:	Open, subject to entry requirements
Course code:	FBB

PERSONS/ROLES

Head of Study Programme
Prof.ssa Sabrina Gaito

Degree Course Coordinator
Prof.ssa Pierangela Samarati

Tutors - Faculty
TUTOR PER L'ORIENTAMENTO:
Valentina Ciriani
Fabio Scotti

Degree Course website
https://sicurezzainformatica.cdl.unimi.it/

Via Celoria 18 - 20133 Milano https://di.unimi.it/it/dipartimento/organizzazione/commissioni Email: orientamento@di.unimi.it
Via Celoria 18 - 20133 Milano https://di.unimi.it/it/dipartimento/organizzazione/commissioni Email: ammissioni.magistrali@di.unimi.it
Via Celoria 18 - 20133 Milano https://di.unimi.it/it/dipartimento/organizzazione/commissioni Email: piani.studio@di.unimi.it
Via Celoria 18 - 20133 Milano https://di.unimi.it/it/dipartimento/organizzazione/commissioni Email: orientamento.uscita@di.unimi.it
Via Celoria 18 - 20133 Milano https://di.unimi.it/it/dipartimento/organizzazione/commissioni Email: tesi.magistrali@di.unimi.it
Via Celoria 18 - 20133 Milano https://di.unimi.it/it/dipartimento/organizzazione/commissioni Email: erasmus@di.unimi.it
Via Celoria 18 - 20133 Milano https://di.unimi.it/it/dipartimento/organizzazione/commissioni Email: trasferimenti@di.unimi.it
Email: rappresentanti.studenti@di.unimi.it

Via Celoria 18 - 20133 Milano Phone 0250316250/252 Sportello su appuntamento (ufficio.didattica@di.unimi.it)
https://di.unimi.it/it/dipartimento/segreterie-e-servizi/ufficio-la-didattica https://informastudenti.unimi.it/saw/ess?AUTH=SAML
Via Celoria 18 - 20133 Milano Phone 0250325032 https://www.unimi.it/it/node/360 https://www.unimi.it/it/node/359/

CHARACTERISTICS OF DEGREE PROGRAMME

General and specific learning objectives

The Master's Degree in Cybersecurity aims to provide solid scientific, methodological and technological foundations for carrying out research, design, implementation, verification, coordination and management of computer systems relating to the various fields of application of computer science and technology in the field of security and protection of systems, networks and computer infrastructures, and the secure and confidential processing of data. The Master's Degree graduate in Cybersecurity carries out design, implementation, verification, usability, maintenance, control and management of secure and protected computer systems and infrastructures. The fundamental objective of his activity is the constant improvement of secure and protected computer systems, also with reference to the secure management of sensitive data, accompanied by the ability to understand and propose in the application fields in which he operates the innovations that continually characterize the discipline.

The training path is aimed at creating professionals with high-level scientific and technological skills, methodological and operational skills and an open and critical vision of the problems connected to the adoption and use of information

technologies, with particular reference to the use of scientific and technological solutions relating to cybersecurity.
The educational objectives described above are acquired through participation in lectures, personal study and classroom or laboratory exercises. Graduates who have sufficient credits in appropriate groups of disciplinary sectors will be able to access the teaching profession in secondary schools, according to the provisions in force.

Expected learning outcomes

Knowledge and understanding
Acquisition of advanced level knowledge and skills in the various areas involved in the security of complex computer systems and data protection.
- Knowledge of scientific, methodological, and technological aspects for the protection of sensitive data.
- Knowledge of scientific, methodological, and technological aspects for the development of secure computer networks and systems.
- Knowledge of scientific, methodological, and technological aspects for the development of secure applications.
- Knowledge of business, economic, and legal aspects related to the management of cybersecurity and data protection.
- Knowledge of scientific, methodological, and technological aspects for the analysis, usability, and verification of the security of computer systems and networks.
Such knowledge and skills are acquired through theoretical lessons and practical exercises and assessed at the end of the courses and the entire course of study. The assessment of individual learning results from a combination of factors inherent to the acquisition of methodological and technological knowledge and skills in the field of cybersecurity and its applications.

Applying knowledge and understanding
Application of knowledge and skills in the analysis, design, implementation and evaluation of secure and protected computer systems operating in different application areas.
- Ability to analyze data protection issues and to identify and implement appropriate methods and techniques for their solution.
- Ability to design, implement and manage secure computer networks and systems.
- Ability to design, develop and manage secure applications.
- Ability to analyze and evaluate aspects of cybersecurity and data protection in different contexts, such as public and private corporate/administrative contexts, including in technological innovation contexts.
Such knowledge and skills are acquired through theoretical lessons and practical exercises and assessed at the end of the courses and the entire course of study. The assessment of individual learning results from a combination of factors inherent to the acquisition of methodological and technological knowledge and skills in the field of cybersecurity and its applications.

Making judgements
Acquisition of a full capacity for autonomous and conscious judgment regarding decisions and design choices in the field of cybersecurity and the possible ethical implications of one's professional activities.
- Autonomy in the analysis of problems (both theoretical and practical) in order to identify the key points for their modeling and resolution.
- Ability to critically and systematically reason, knowing how to independently develop a study or research plan for the resolution of complex problems.
- Ability to read and critically and objectively evaluate the results obtained from appropriate experiments, or described in technical-scientific reports and in scientific literature.
- Autonomy in the design, development and analysis of systems, networks, infrastructures and applications in the field of cybersecurity.
- Ability to evaluate the economic, ethical, legal, social and environmental implications of digital transformation.
Such knowledge and skills are acquired through theoretical lessons and practical exercises and assessed at the end of the courses and the entire course of study. The assessment of individual learning results from a combination of factors relating to the acquisition of methodological and technological knowledge and skills in the field of cybersecurity and its applications.

Communication skills
Acquisition of relational and communication skills to enable the management and promotion of cybersecurity in various application areas, including interdisciplinary ones.
- Ability to present and critically evaluate in writing, in a clear, coherent and concise manner, technical and methodological ideas and arguments, using appropriate technical terminology and language.
- Ability to formulate and express orally, even in public contexts, complex arguments regarding methodologies and technologies related to cybersecurity.
- Ability to elaborate in a complete and coherent manner an original research dissertation on a complex topic, also through the use of appropriate technological supports.
Such knowledge and skills are acquired through theoretical lessons and practical exercises and assessed at the end of the courses and the entire course of study.

Learning skills
Acquisition of autonomous organizational skills that allow continuous updating of knowledge.
- Ability to use libraries, databases, archives and paper and electronic repertoires to access scientific information and relevant sources.

- Ability to identify a problem and identify the analysis and research activities necessary to reach a solution.
- Ability to update skills and abilities, to keep constantly updated with the continuous advances in computer science and cybersecurity, so as to adapt to new situations and types of problems.

Such knowledge and skills are acquired through theoretical lessons and practical exercises and assessed at the end of the teachings and the entire course of study, in particular through the carrying out of in-depth methodological and technological studies.

Professional profile and employment opportunities

Specialists in the design and management of secure IT networks and infrastructures

Role in a work context

Experts in advanced cybersecurity issues related to the design, configuration and management of IT networks and infrastructures for critical systems and resources. These professional figures deal with technological aspects for which an extremely in-depth knowledge of the technologies and evolutionary trends for cybersecurity at a global level is required. They are therefore indispensable in cases where the ability to analyze highly complex and specific technological scenarios is required, including architectures based on IoT, cyber-physical systems, cloud/fog/edge computing, mobile architectures and data intensive architectures.

Skills associated with the role

These professional figures are advanced level specialists who have studied in particular all the aspects, even the most detailed ones, of the scientific, methodological, technological and application aspects of cybersecurity in networks and infrastructures. Advanced skills of this type are required for the detection, analysis, defense and prevention of intrusions, cyber attacks and malware.

Career opportunities

They carry out specialized professional activities in the field of design and management of secure IT networks and infrastructures. This activity may be carried out, even as a freelancer, in all areas of the private and public sector that operate in the design, development, management, maintenance or use of IT networks and infrastructures in a wide range of sectors, including information and communication technologies and all application sectors that use them. This activity may also be carried out in research institutions and universities as technical support for research and experimentation activities in the fields of knowledge and skills of this professional profile.

Specialists in the design and management of solutions for the secure processing and protection of data

Function in a work context

Experts in advanced data protection issues in the context of data management, analysis and sharing. These professional figures address issues that require extremely in-depth knowledge of the scientific, methodological, technological and applicative aspects related to data security and privacy. They are therefore indispensable in cases where the ability to analyze highly complex and specific scenarios is required, including IoT, cyber-physical, cloud/fog/edge, mobile and data-intensive architecture scenarios.

Skills associated with the role

These professional figures are advanced level specialists who have studied in particular all the aspects, even the most detailed ones, of the scientific, methodological, technological and application aspects of data security and privacy. Advanced skills of this type are required to ensure the management, analysis, use and sharing of data, guaranteeing its protection.

Career opportunities

They carry out specialized professional activities in the field of design and management of solutions for the secure processing of data that are increasingly necessary in the modern digital society based on the collection, sharing, and analysis of large collections of data and which therefore requires guarantees of correct protection and use of data in compliance with legislation, regulations, and protection requirements by citizens, businesses and companies. This activity may be carried out, even as a freelancer, in all areas of the private and public sector that operate in the design, development, management, maintenance or use of information systems, applications, or data processing scenarios in a wide range of sectors, including information and communication technologies and all application sectors that use them. This activity may also be carried out in research institutions and universities as technical support for research and experimentation activities in the areas of knowledge and skills of this professional profile.

Specialists in the design and management of IT systems, information systems and applications with security and privacy guarantees

Function in a work context

Experts in advanced cybersecurity issues relating to both the systems and critical resources of a company (data centers, high-reliability systems, intellectual property, sensitive data) and those arising from the most innovative technological solutions. These professional figures deal with technological aspects for which an extremely in-depth knowledge of technologies and evolutionary trends at a global level is required. They are therefore indispensable in cases where the ability to analyze highly complex and specific technological scenarios is required.

Skills associated with the role

These professional figures are advanced level specialists who have studied in particular all the aspects, even the most detailed ones, of some innovative technologies. Advanced skills of this type may be required in all typical areas of cybersecurity, from secure programming with the application of advanced static and dynamic analysis methodologies, the analysis of malicious code continuously released on the Internet, advanced encryption techniques, advanced techniques for protecting data and ensuring their security and confidentiality, advanced artificial intelligence techniques with consideration

of their security as well as the application of such techniques in security solutions and testing and monitoring methodologies of innovative applications.

Career opportunities

The information technology sector is characterized by the presence in many companies, both large and small but highly specialized, as well as in the consulting sector, of technological excellence that involves the continuous research and application of the most innovative solutions. In all these cases, the management of corporate information systems requires highly specialized professionals capable of dealing with complex scenarios in which technologies that present highly difficult problems are used. This activity may be carried out, even as a freelancer, in all areas of the private and public sector that operate in the design, development, management, maintenance or use of computer and information systems, or applications in a wide range of sectors, including information and communication technologies and all application sectors that use them. This activity may also be carried out in research institutions and universities as technical support for research and experimentation activities in the areas of knowledge and skills of this professional profile.

Information and communication technology specialists

Function in a work context

The professions included in this category belong to the professional profiles of experts in the use, in various operational contexts, of the information and communication technologies, on which the LM-66 course of study is largely based.

These professional figures integrate the ability to develop sophisticated IT applications with knowledge of operational issues in various application contexts (including IoT, cloud/fog/edge computing and data intensive architectures) by designing, managing and maintaining complex and articulated IT applications.

Skills associated with the function

These professional figures possess excellent fundamental knowledge and a broad spectrum of knowledge and skills in the various sectors of IT, are familiar with the scientific method of investigation, have high modelling skills, know how to understand and use mathematical tools to support IT skills, are able to manage group activities, operate autonomously and fit in quickly in work environments.

Career opportunities

Graduates can work in the most varied application areas for the design and management of complex IT systems and for the study and research of new systems and applications. This activity can be carried out, even as a freelancer, in all areas of the private and public sector that operate in the design, development, management, maintenance or use of IT systems, or applications in a wide range of sectors, including information and communication technologies and all the application sectors that use them. This activity can also be carried out in research institutions and universities as technical support for research and experimentation activities in the areas of knowledge and skills of this professional profile.

Initial knowledge required

The following may access the master's degree course:

- graduates of the degree class in Computer Science and Technology (L-31) and of the corresponding class relating to Ministerial Decree 509/99;
- graduates of other classes provided that they have acquired at least the following in their previous studies:

48 credits in the INF/01 or ING-INF/05 sector

12 credits in the MAT/01- 09 sectors

The degree course may also be accessed by those in possession of another qualification obtained abroad and recognized as suitable on the basis of equivalence who have acquired skills and knowledge equivalent to those of the above-mentioned requirements.

To verify the curricular requirements and personal preparation, the candidate must provide the following documents: degree certificate with grade, list of exams passed with grade and number of credits.

Verification of the adequacy of personal preparation will be based on the results reported in the exams of the scientific-disciplinary sectors indicated among the access requirements. When this does not demonstrate the full adequacy of the personal preparation, the candidate will also be required to pass an individual interview.

Compulsory attendance

Attendance is strongly recommended for both courses and laboratories.

Degree programme final exams

Once the necessary training credits have been acquired in compliance with the regulations, the student is admitted to take the final exam to obtain the degree. In compliance with the general criteria expressed in the University Teaching Regulations, the final exam consists in the writing of a thesis related to a theoretical or experimental activity carried out independently by the student, under the supervision of one or more professors, in research groups or companies; the thesis must document the design and implementation aspects of the activity carried out as well as the connections of the work with the current state of knowledge in the field of cyber security.

Campus

IT course venues: via Celoria 18 - Milan.

Other course venues: Teaching sector, via Celoria 20; Teaching sector, via Golgi 19; Teaching sector, via Venezian 15.

Laboratories

Computer laboratory (Silab) at the Department of Computer Science, via Celoria 18, Milan.

Notes

In order to obtain their degree, students must be proficient in English at a B2 level under the Common European Framework of Reference for Languages (CEFR). This proficiency level may be certified as follows:
- By submitting a language certificate attesting B2 or higher level in English and issued no more than three years before the date of submission. You will find the list of language certificates recognized by the University at: https://www.unimi.it/en/node/39322. The certificate must be uploaded during the enrolment procedure, or subsequently to the portal http://studente.unimi.it/uploadCertificazioniLingue;
- By taking a placement test offered by the University Language Centre (SLAM) between October and January of the first year. Students who fail the test will be required to take a SLAM course.

The placement test is mandatory for all those who do not hold a valid certificate.
Those who have not taken the placement test by the end of December or fail the end-of-course exam six times must obtain the necessary certification privately before graduating.

EXPERIENCE OF STUDY ABROAD AS PART OF THE TRAINING PROGRAM

The University of Milan supports international mobility by providing its students with the opportunity to spend study and internship periods abroad. It is a unique chance to enrich your educational path in a new exciting environment.

The agreements entered into by the University with over 300 universities from the 27 EU member countries under the European Erasmus+ programme allow regularly enrolled students to carry out part of their studies at one of the partner universities or to undertake internships at companies, training and research centres and other organisations.

Similar international mobility opportunities are provided outside Europe, through agreements with a number of prestigious institutions.

The University of Milan is a member of the 4EU+ European University Alliance that brings together eight public multidisciplinary universities: University of Milan, Charles University of Prague, Heidelberg University, Paris-Panthéon-Assas University, Sorbonne University of Paris, University of Copenhagen, University of Geneva, and University of Warsaw. The 4EU+ Alliance offers integrated educational pathways and programmes to promote the international mobility of students (physical, blended and virtual).

Study and internships abroad

The education program can be enriched by educational activities abroad both to deepen some topics and as socialization experience in international environments. Within the Erasmus+ program study periods can be taken in over 50 universities in Belgium, Czech Republic, Finland, France, Germany, Greece, Hungary, Lithuania, Norway, Netherlands, Poland, Portugal, Romania, Slovenia, Spain, Switzerland, Turkey. Courses will be recognized in the personalized study plan. These periods abroad are typically 5-month long and include courses for about 30 CFU, in the area of information and communication technology and related applications. Recognition of these educational activities will be based on the Learning Agreement, to be defined in advance by the student and the Erasmus coordinator at the Computer Science Department before starting the period abroad: course in the learning agreement with passed exams will replace the educational activities of the study plan ("manifesto"), either by covering the same topics or complementing the acquired basic competences. The Erasmus Committee at the Computer Science Department will perform the recognition of CFU obtained abroad and the definition of the personalized study plan. Similarly, stages to prepare the final dissertation are allowed in the same foreign universities. Recognition will be performed by the Department Erasmus Committee.
Erasmus: the coordinator for the Department of Informatics is Prof. Fabio Scotti.
International Programs: the coordinator for the Department of Informatics is Prof. Davide Rocchesso.
More information are available at the following link: https://di.unimi.it/it/rapporti-internazionali/mobilita-internazionale/opportunita-internazionali

How to participate in Erasmus mobility programs

The students of the University of Milan can participate in mobility programmes, through a public selection procedure.
Ad hoc commissions will evaluate:
- Academic career
- the candidate's proposed study programme abroad
- his/her foreign language proficiency
- the reasons behind his/her application

Call for applications and informative meetings
The public selection for Erasmus+ mobility for study generally begins around February each year with the publication of a call for applications specifying destinations and requirements. Regarding the Erasmus+ Mobility for Traineeship, the University of Milan usually publishes two calls a year enabling students to choose a destination defined by an inter-institutional agreement or to find a traineeship position on their own.

The University organises informative meetings to illustrate mobility opportunities and rules for participation.

Erasmus+ scholarship
The European Union grants the winners of the Erasmus+ programme selection a scholarship to contribute to their mobility costs, which may be supplemented by the University funding for disadvantaged students.

Language courses
Students who pass the selections for mobility programmes can benefit from intensive foreign language courses offered each year by the University Language Centre (SLAM).
https://www.unimi.it/en/node/8/

Learn more at https://www.unimi.it/en/node/274/

For assistance, please contact:
International Mobility Office
Via Santa Sofia 9 (second floor)
Tel. 02 503 13501-12589-13495-13502
Contacts: InformaStudenti;
Student Desk booking through InformaStudenti

1st COURSE YEAR Core/compulsory courses/activities common			
Learning activity		**Ects**	**Sector**
ARTIFICIAL INTELLIGENCE FOR SECURITY AND PRIVACY		6	INF/01
CRYPTOGRAPHY		6	INF/01
English proficiency B2 (3 ECTS)		3	NN
NETWORK SECURITY		6	INF/01
PRIVACY AND DATA PROTECTION		6	INF/01
SECURE DATA MANAGEMENT		6	INF/01
SECURITY OF DATA-INTENSIVE ARCHITECTURES		6	INF/01
SOFTWARE PROTECTION TECHNIQUES		6	INF/01
	Total compulsory credits	45	
Elective courses			
BIOMETRIC TECHNIQUES AND APPLICATIONS		6	INF/01
CYBERSECURITY MANAGEMENT IN BUSINESSES		6	SECS-P/08
DEPENDABILITY		6	INF/01
DIGITAL FORENSICS		6	INF/01
MACHINE LEARNING FOR SYSTEMS AND NETWORK SECURITY		6	INF/01
SPECIFICATION AND VERIFICATION OF CRITICAL SYSTEMS		6	INF/01
2nd COURSE YEAR (available as of academic year 2026/27) Core/compulsory courses/activities common			
Learning activity		**Ects**	**Sector**
LEGAL BASIS FOR SECURITY AND PRIVACY		6	IUS/20
RISK ANALYSIS AND MANAGEMENT		6	SECS-S/01
	Total compulsory credits	12	
Elective courses			
CYBERSECURITY IN OPERATING SYSTEMS		6	INF/01
DEFENSIVE (CYBER)SECURITY		6	INF/01
QUANTUM AND POST-QUANTUM COMPUTING		6	INF/01
Further elective courses			