UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CONSIGLIO INTERCLASSE IN MATEMATICA

COURSE OF STUDY TWO-YEAR MASTER OF SCIENCE PROGRAMME IN MATHEMATICS

ACADEMIC YEAR 2023-2024

ACADEMIC SUBJECT CRYPTOGRAPHY

General information	
Programme year	Second
Term	Second semester (February 26, 2024 – May 31, 2024)
European Credit Transfer and Accumulation System credits (ECTS)	7
SSD	MAT/02 – Algebra
Language	Italian
Mode of attendance	Not mandatory

Lecturers	
Name and surname	Roberto La Scala
E-mail	roberto.lascala@uniba.it
Telephone	+39 080 544 2674
Department and office	Department of Mathematics, room 28 second floor
Virtual meeting room	Microsoft Teams: Crittografia, code 8ge6u5g
Web page	https://www.dm.uniba.it/it/members/lascala
Office hours	Mon. Wed. Fri. 12:00 – 13:00, in presence or online (by appointment)

Work schedule				
	Total	Lectures	Hands-on learning	Self-study
Hours	175	56		119
ECTS credits	7	7		

Learning objectives	
	Knowledge of the concepts and methods of modern cryptography.

Course prerequisites	
	The knowledge that is typically acquired in the three years of a degree of L-35 class. In particular: arithmetic, algebraic structures and discrete probability.

Syllabus	
Course contents	Classic cryptography, cryptanalysis. Shannon's information theory, perfect secrecy, information entropy, key-equivocation. Product ciphers, block ciphers, Data Encryption Standard, Advanced Encryption Standard. Public key cryptography, RSA cryptosystem, primality tests, square roots modulo n, factorization algorithms. Discrete logarithms, ElGamal's cryptosystem, computation of discrete logarithms. Applications of cryptography to digital signature.
Reference books	D. Stinson, Cryptography: theory and practice, 3rd Edition, 2005 S. Vaudenay, A classical introduction to cryptography, Springer, 2006
Additional course materials	Implemented algorithms in the programming language of SageMath.
Repository	Microsoft Teams

Expected learning outcomes	
Knowledge and understanding	Knowledge of the ideas that allowed the development of the main ciphers used in modern cryptography and their cryptanalysis.
Applying knowledge and understanding	The general theory acquired during the course is used for the implementation and analysis of the presented ciphers.
Soft skills	*Making judgements*: Ability to evaluate the correctness of the methods presented. Ability to identify suitable tools to address information confidentiality problems.
	Communication skills: Acquisition of the algorithmic language, necessary for the understanding, analysis and presentation of the methods inherent to cryptography and cryptanalysis.
	Learning skills: Acquisition of an adequate study method, supported by the implementation of the algorithms and ciphers proposed during the course.

Teaching methods	
	Lectures and programming sessions

Assessment	
Assessment methods	Oral final exam
Evaluation criteria	• *Knowledge and understanding*: • *Applying knowledge and understanding*: • *Making judgement*: • *Communication skills*: • *Learning skills*:
Grading policy	Final evaluation expressed in 30th and exam passed with at least 18 over 30.

Further information	
	Attendance at lectures and tutorials is strongly recommended.