



Master's Program in Coding Theory and Information Storage

Description

As society becomes increasingly data-driven, the ability to store, transmit, and protect information reliably has become a fundamental requirement of modern digital infrastructures. From cloud computing and telecommunications to distributed storage systems and artificial intelligence, ensuring the integrity, availability, and efficiency of information is a major scientific and technological challenge. The rapid evolution of information technologies, coupled with the exponential growth of digital data, creates an increasing demand for specialists capable of developing advanced methods for reliable information processing and storage.

The Master's Program in **Coding Theory and Information Storage** provides students with a strong foundation in the mathematical principles and engineering techniques that underpin modern communication and storage systems. The program combines rigorous theoretical training with practical applications, preparing graduates to address challenges related to error correction, data compression, information security, and large-scale storage architectures.

Relevance to the Job Market

Graduates are well prepared for careers in research and development, telecommunications, cloud computing, data storage, cybersecurity, software engineering, and high-performance computing. They can contribute to the design and optimization of reliable communication systems, distributed storage infrastructures, and data-intensive applications in sectors such as information technology, telecommunications, finance, healthcare, manufacturing, and public administration. The program also provides an excellent foundation for doctoral studies and academic research in information theory, applied mathematics, computer science, and electrical engineering.

Competencies Acquired

Upon completion of the program, graduates will be able to:

- Development of cryptographic algorithms and protocols — designing and implementing algorithms and protocols used for information confidentiality, integrity, and authentication
- Development of cryptographic modules — building software/hardware components that implement cryptographic functions for real-world systems



National University of Science and Technology
POLITEHNICA Bucharest
Faculty of Applied Sciences



- Security evaluation of IT products — assessing information systems and products against security requirements and standards
- Cryptographic security evaluation — analyzing the robustness and correctness of cryptographic implementations
- Cryptanalysis — techniques and methods for analyzing and breaking cryptographic schemes
- IT security audit — reviewing and assessing the security posture of information systems and communication infrastructures
- Building IT security solutions — designing and implementing practical security solutions for computer and communication systems

Selected Courses

The curriculum includes advanced topics such as:

- Information compression
- Computer crime / cybercrime
- Cryptology (cryptography and cryptanalysis)
- Cybersecurity
- Security of computer and communication systems
- Protection against malicious applications

Research Topics

Students have the opportunity to participate in research projects in areas including:

- Blockchain technologies
- Anti-malware protection techniques and methods
- Critical infrastructure protection
- Digital forensics — techniques and methods for digital evidence investigation
- Cryptanalysis techniques and methods
- Digital identity management and access control systems
- Blockchain-based document management applications
- Solutions for extracting information from Darkweb networks



National University of Science and Technology
POLITEHNICA Bucharest
Faculty of Applied Sciences



- Honeypot systems for intercepting and analyzing malware exfiltration traffic
- Software for identifying message types transmitted through encrypted public messaging applications
- Real-time intrusion detection solutions for security incident management
- Cybersecurity risk management
- Threat management
- Machine learning algorithms applied to cybersecurity
- AI-based solutions for predictions in the cybersecurity domain

Additional Information

- **Language of instruction:** Romanian
- **Duration:** 2 years
- **Degree awarded:** Master of Science (M.Sc.) in Applied Engineering Sciences
- **Contact person:** Conf .dr. Emil SIMION, emil.simion@upb.ro
- **Web page:** <https://www.tcsi.ro/>, <https://masterat.upb.ro/masterate/www.tcsi.ro>