|  |
| --- |
| **Topics** |

|  |
| --- |
| **Computer Science (5)** |

|  |  |
| --- | --- |
|  |  |
| **Industrial Applications** | This topic studies measurement and control technologies, robotics and automation in industrial networks. This topic includes communication protocols and technologies such as ZigBee, Bluetooth, PLC, HAPS, and RFID which are also closely related to SCADA, Smart Factories, Smart Cities, Smart Grid and Smart Industry ecosystems. |
|  |  |
| **Communication Theory** | Communication theory studies principles and methods by which the information is transmitted. The topic covers information theory (Shannon theory, entropy), information source and discrete communication systems. In particular, description of data and signal structures, transmission and modulation methods, redundancy reducing and signal processing are provided. |
|  |  |
| **Computer Networks** | This topic studies the structure of the computer networks and communication protocols. The main topics are network protocol models (ISO/OSI, TCP/IP), routing, switching, network services (NAT, DHCP, DNS), wireless and mobile networks (Wi-Fi, GSM, LTE, 5G), database and web services. |
|  |  |
| **Quantum computing** | Quantum computing studies the main algorithms that can be run in a quantum computer. Main topics: Tensor-product, entanglement, qubits, Grover’s search algorithm, Shor's algorithm, and quantum secret key distribution. |
|  |  |
| **Theoretical Computer Science** | This topic studies how to develop efficiently an algorithm with the required specifications. Examples of algorithms treated in this topic are: sorting numbers, parallel and sequential algorithms, distributed algorithms, optimization, and genetic algorithms. Data structures such as arrays, records and objects are also introduced. |
|  |  |

|  |
| --- |
| **Cryptology (4)** |

|  |  |
| --- | --- |
|  |  |
| **Advanced Cryptology** | This topic focuses on modern cryptographic protocols and technologies, i.e. crypto-currency (e.g., bitcoins and Etherium), elliptic curve cryptography (e.g., EC Diffie-Hellman protocol, Boneh and Franklin’s IBE Scheme and the MOV attack), secure multiparty computation, secret sharing, homomorphic encryption and searchable encryption. |
|  |  |
| **Cryptanalysis** | This topic studies the properties of a cryptographic protocol such as indistinguishability or unforgeability, and the possible attacks that a protocol can receives as chosen ciphertext-attack or man in the middle attack. |
|  |  |
| **Fundamental Cryptology** | Basic background in cryptology: history of cryptology (e.g., Cesar cipher and Vigenere cipher), symmetric and asymmetric cryptography (stream and block ciphers, certificates, PKI), authentication, authorization, and pseudo-random number generators. |
|  |  |
| **Post-quantum Cryptography** | This topic studies that kind of cryptographic protocols which are secure against a quantum computer. Main topics are: lattice-based cryptography (e.g., SVP, CVP, SIVP, LWE and R-LWE problems), multivariate cryptography (i.e., asymmetric cryptography based on non-linear multivariate polynomials over finite fields) and coding theory (e.g., linear codes, parity-check matrices, and syndrome decoding tables). |
|  |  |

|  |
| --- |
| **Humanistic and Social Science (4)** |

|  |  |
| --- | --- |
|  |  |
| **Cybercrime** | Cybercrime revises the literature in computer crime, in particular, it focuses on computer misuse, data protection, criminal damage, software privacy, forgery, and investigative powers which lead to expansion of the internet, pornography, unsuitable material, and social engineering. |
|  |  |
| **Human Aspects of Security and Privacy** | This topic studies the cultural, societal, political, psychological, and ethical implications of information security and privacy. For example, how to develop approaches that ensure that individuals make informed decisions about security and privacy. |
|  |  |
| **Security Architecture** | Study the design and implementation of security architectures, i.e. analyze governance, risk and compliance issues related to architectures and see how organizations manage their security policies. |
|  |  |
| **Security Management** **and Risk Analysis** | This topic focuses on the identification of organization's assets and, therefore, the implementation of policies and procedures for protecting these assets.  It also considers law regulations, obligations and liabilities between private parties, and the implications of government regulations for corporate risk management. |
|  |  |

|  |
| --- |
| **Mathematics (5)** |

|  |  |
| --- | --- |
|  |  |
| **Algebra and Discrete Mathematics** | *Algebra* studies the basic algebraic structures such as groups (and congruence), rings and fields (in particular, finite fields); with a focus on irreducible polynomials over finite fields, extensions and Galois theory.  *Discrete mathematics* studies discrete (non-continuous) structures such as partially ordered sets, graphs and codes; and deals with counting over these finite structures, e.g. methods of counting, principle of inclusion and exclusion and integer partitions. |
|  |  |
| **Complexity Theory** | Complexity theory is the study of the complexity of problems and algorithms. In particular, this topic defines algorithms, Turing machines, and the concept of computational hardness. The classification of decision problem (e.g., P, NP, NP-complete) is also presented. |
|  |  |
| **Number Theory** | Number theory studies integers, in particular, prime numbers, primality tests and factorization considering the complexity of the studied algorithms. More in specific, Diophantine equations, elliptic curves, binary quadratic forms and quadratic number fields are also considered. |
|  |  |
| **Probability and Statistics** | *Probability* focuses on random variables, distributions and density functions. This topic also deals with stochastic processes, probabilistic methods used to model systems, method of conditioning and Markov chain.  *Statistics* deals with the collection and the analysis of data. Its main methods are parametric estimation, hypothesis testing and regression analysis. It also deals with multivariate analyses such as data exploration, modeling and inference. |
|  |  |
| **Topology and Analysis** | *Topology* studies the properties of space that are preserved under continuous deformations (e.g., knot theory, metrics, metric space, quotient and product spaces). *Analysis* deals with limits, differentiation, integration, analytic functions and series. |
|  |  |

|  |
| --- |
| **Privacy (3)** |

|  |  |
| --- | --- |
|  |  |
| **Data Extraction** | Data mining goal is to extract information from a data set which can be used for future purposes. It involves machine learning, statistics and database systems. Main topics: cluster analysis and anomaly detection. |
|  |  |
| **Data Privacy** | This topic focuses on data processing (e.g., validation, sorting or aggregation) and statistical disclosure control (SDC) methods which aim at releasing data (i.e., data set, data base or tabular) that preserve their statistical validity while protecting the privacy of each data subject. Examples of SDC methods are suppression, generalization, data swapping and microaggregation. Privacy models such as k-anonymity and differential privacy are also introduced. |
|  |  |
| **Privacy-enhancing Technologies** | Privacy-enhancing technologies are cryptographic methods dealing with guarantee the user’s privacy in accordance with the law. This topic studies cryptographic protocols such as group and ring signatures, and anonymous credentials. Further, PETs may cover privacy protection protocols and tools, e.g. ToR, onion routing, proxies, anonymous search engines, anonymous instant messaging etc. |
|  |  |

|  |
| --- |
| **Security (4)** |

|  |  |
| --- | --- |
|  |  |
| **Hardware and Software Security** | This topic focuses on existing secure hardware devices (e.g. smart cards), HW and SW implementation of cryptographic algorithms (e.g. Intel and Atmel crypto accelerators), vulnerabilities, possible attacks and known weaknesses., i.e. side channels attacks (timing and power analyses), masking, backdoors, implementation errors, data eavesdropping, skimming etc.) and hardware and software design. |
|  |  |
| **Network Security** | This topic presents approaches to the prevention, detection, mitigation, and remediation of security problems in the network at each layer. Main topics: Virtual Private Networks (VPN), TLS, firewalls, IDS (Intrusion Detection System), Intrusion Prevention Systems (IPS), cloud security, web security and penetration testing. |
|  |  |
| **Security systems** | Security systems study systems which are designed for the protection of assets of individuals and institutions. Examples are Intruder Alarm Systems (IAS), Fire Alarm Systems (FAS), Closed-circuit televisions (CCTV) or Access control systems (password-, card- and biometric based). The topic includes secure industrial control systems (e.g., SCADA, PLC, RFID) and embedded systems. |
|  |  |
| **System Security** | This topic presents different techniques for the design and implementation of secure applications. Main topics: secure programming (algorithm design and algorithm efficiency), operating systems (e.g. Windows, Linux, OSX, Android), malware, SELinux, security measures (e.g., anti-virus, anti-malware, firewall), digital forensics and SW virtualization. |
|  |  |