MODULE DESCRIPTION CARD – SYLLABUS

This module is a part of the Intensive International Education Programs in the field of the … organised at Poznan University of Technology as part of the „IMPACT – Innowacyjne Międzynarodowe Programy w AI, Cyberbezpieczeństwie i Teleinformatyce" project implemented SPINAKER Program of the National Agency for Academic Exchange, financed by the European Social Development Fund 2021–2027 (ESDF).

Module name:	Number of hours:	Lecturer:
Cybersecurity in a Post-Quantum World	10	Anna Grocholewska-Czuryło, PhD

Module Descriptions:

The module introduces students to the foundations of post-quantum cryptography (PQC) and quantum-safe security, including the impact of quantum computing on current cryptographic systems and global cybersecurity. It covers the basic principles of quantum computation relevant to security, quantum threat models, vulnerabilities of widely used cryptographic algorithms, and the main families of post-quantum schemes. The module also presents current and emerging PQC standards (e.g. NIST), crypto-agile migration strategies, hybrid solutions, and an introductory overview of Quantum Key Distribution (QKD) and its role in future secure communication architectures. Students will gain both theoretical knowledge and practical understanding of how to assess quantum risk, design quantum-safe solutions, and relate technical choices to regulatory, ethical, and societal contexts.

Purpose of the support under Module:

The overall objective of the Innovative International Education Program in Cybersecurity within the IMPACT project is to raise the competencies of international students in key digital technologies and to support personalized, flexible, and modern education aligned with current global needs in the area of cybersecurity.

The specific purpose of this module is to equip students with essential competencies in post-quantum cryptography and quantum-safe security, including:

- understanding how quantum computing affects classical cryptography and global cyber risk,
- learning the main families and design principles of post-quantum cryptographic schemes and standards,
- analyzing and comparing the security and performance of quantum-resistant algorithms and hybrid solutions,
- planning and evaluating migration strategies toward quantum-safe infrastructures in real-world systems,
- developing awareness of the ethical, legal, and strategic implications of quantum technologies, including the role of QKD and long-term data protection.

Method of support under Module:

Support within the module is provided with the participation of the instructor and divided into the following elements:

- 6-week self-study program using teaching materials provided by the instructor on the e-learning platform;
- 6 weeks of support from the instructor in the form of online consultations using tools that enable meetings to be held;
- a test to verify the acquisition of competences.

Module-related learning outcomes:

Descriptions of the new competences:

Participants gain new skills in post-quantum cryptography and quantum-safe security, including knowledge of how quantum algorithms threaten current cryptographic mechanisms, how to classify and understand the main post-quantum cryptographic families, and how to interpret current PQC standards and recommendations. Students also develop the ability to assess quantum-related risks in real systems, design or evaluate migration paths (including hybrid solutions), and understand the role and limitations of QKD in future secure architectures. In addition, they become aware of the ethical, legal and strategic dimensions of quantum technologies and their impact on privacy, critical infrastructures and globally interconnected systems.

Knowledge:

1. Student has structured and theoretically grounded knowledge of quantum threats to classical cryptography, including the impact of key quantum algorithms (e.g. Shor, Grover) on widely used cryptosystems and protocols.
2. Student has structured knowledge of the main families of post-quantum cryptographic schemes (e.g. lattice-based, code-based, multivariate, hash-based) and understands the principles of current PQC standards and hybrid quantum-safe solutions.
3. Student understands development trends and modern achievements in cybersecurity related to post-quantum cryptography, quantum key distribution, and global quantum-readiness strategies, including their technological, regulatory, and societal context.

Skills:

1. Student can critically assess and interpret information from scientific literature, standards, and technical reports regarding post-quantum cryptography, QKD, and quantum-related threats to cybersecurity.
2. Student is able to evaluate and compare selected post-quantum algorithms and migration approaches in terms of security assumptions, performance, implementation constraints, and applicability to specific systems and infrastructures.
3. Student is able to independently continue learning in the field of post-quantum cryptography and quantum-safe security, and to guide others in acquiring new competencies in response to evolving quantum technologies and cryptanalytic capabilities.

Social competences:

1. Student understands that knowledge in IT, cryptography, and quantum technologies evolves rapidly, and therefore recognizes the need for continuous learning, monitoring of standards, and updating of security practices.
2. Student demonstrates ethical and responsible behavior when assessing and applying quantum-safe solutions, taking into account long-term confidentiality, privacy protection, and the potential impact of quantum technologies on society and critical infrastructures.

Criteria for verifying learning outcomes

Learning outcomes are verified through an online single-choice test assessing the student's knowledge of quantum threats, post-quantum cryptographic families and standards, hybrid and migration strategies, the basics of QKD, and the broader implications of quantum-safe security. The test checks both theoretical understanding and the ability to correctly interpret and classify quantum-related security concepts. A minimum of 51% of correct answers is required to pass.

Method of verification/validation of learning outcomes

Verification is carried out using an online single-choice test delivered on the dedicated e-learning platform. The test is conducted individually, without access to supporting materials, and evaluates the extent to which the student has achieved the intended knowledge, skills, and social competences. The results are automatically recorded and validated according to predefined assessment criteria.

Workload

25 h (including work with teaching materials provided by the lecturer, consultation, and the student's own work) – 1 ECTS point

Level of the European Qualifications Framework