Accessible Post-Quantum Cryptography University Syllabus (Focus on Lattice-Based Cryptography)

This course material is meant to help make teaching post-quantum cryptography more accessible to university students who may lack the mathematical and theoretical computer science prerequisite knowledge. Post-quantum cryptography, similarly to classical cryptography, relies on an advanced theoretical and mathematical background, which students lacking the prerequisite knowledge might find overwhelming. The aim of this syllabus is to simplify teaching post-quantum cryptography and, in particular, Lattice-Based Cryptography, which is one of the most popular approaches for constructing post-quantum secure cryptography. This approach itself is a whole course on its own.

To make its teaching accessible to general computer science students, we have provided slides along with guidance on what should be taught and the key takeaway points. Additionally, we have included a practical sheet on using the SageMath software to help understand and implement these mathematical concepts. We have incorporated intuitive explanations for complex mathematical constructs, which we hope will aid both instructors and students.

1 CyBOK Mapping

The course material maps to the following knowledge areas of the CyBOK:

- **Systems Security → Cryptography**
- **Infrastructure Security → Applied Cryptography**

2 Lecture Slides

A summary of the provided material can be found below. The material is available in both Interactive Display mode (best viewed in full-screen mode using Adobe Acrobat Reader) and handout mode (4x1 sheets).

- **Introduction**: Provides a general introduction to post-quantum cryptography and why classical cryptography is vulnerable to quantum attacks.
  Suggested Duration: 1-2 hours.
- **Introduction to Lattices**: Provides an intuitive and comprehensive introduction to this mathematical structure and related concepts.
  Suggested Duration: 2-3 hours, depending on the background knowledge of the students.
- **Introduction to Lattice-related Hard Problems**: Covers lattice-related hard problems that are used in lattice-based post-quantum cryptography.
  Suggested Duration: 1-2 hours, depending on the background knowledge of the students.

- **Introduction to Public-Key Cryptography from Lattices**: Provides coverage of some lattice-based public key encryption schemes.
  Suggested Duration: 1-2 hours, depending on the background knowledge of the students.

- **Digital Signatures and Hash Functions from Lattices**: Provides an intuitive and comprehensive overview of approaches for constructing hash functions and digital signatures from lattices.
  Suggested Duration: 1-2 hours, depending on the background knowledge of the students.

3 Practical Material

We have provided a comprehensive sheet showing how to use SageMath software to practice and implement complex mathematical concepts related to Lattice-Based post-quantum cryptography. The sheet covers the core mathematical constructs and related concepts.

SageMath is a powerful open-source mathematics software system licensed under the GNU General Public License (GPL). It integrates a wide range of mathematics tools into one unified interface and is built on top of many open-source packages.

More information about SageMath can be found on its official website: https://www.sagemath.org.