

(1.) Course Title: INFPHD452 Mathematical methods in cryptography	Credits: 6
Course Classification: Optional	
Theoretical or Practical Nature of the Course, 'training character'¹³: 80%-20% (credit%)	
Type of Class: lecture and number of hours: 2/week in the given semester, <i>(If the course is not (only) taught in Hungarian, then the language: English)</i> Additional (specific) methods and characteristics² used in delivering the knowledge <i>(if any)</i> : -	
Assessment Method (Exam / Midterm Grade / Other³): colloquium Additional (specific) methods⁴ applied in knowledge assessment <i>(if any)</i> : -	
Course Placement in Curriculum (Semester Number): -	
Prerequisites <i>(if any)</i> : -	
Course Description: A concise yet informative description of the knowledge to be acquired.	
The course covers several mathematical methods related to well-known and unorthodox cryptographic methods and applications. The main goal is to present the underlying theoretical methods behind the particular cryptographic protocols and show non-trivial connections between various aspects. The main topics of the course: • elliptic curve cryptography • lattice based cryptography • cryptosystems based on number theoretic arguments secret sharing	
2-5 Most Important Required and Recommended Literature List of required and recommended literature (notes, textbooks) with bibliographic data (author, title, publication details, (possibly pages), ISBN).	
1. Ronald Cramer, Ivan B. Damgaard, Jesper B. Nielsen: Secure Multiparty Computation and Secret Sharing, Cambridge University Press, 2015 2. Darrel Hankerson, Alfred Menezes, and Scott Vanstone: Guide to Elliptic Curve Cryptography, Springer, 2004 3. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman: An Introduction to Mathematical Cryptography, Springer 2014 4. Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography, Chapman & Hall/CRC, 2021	
List of Prescribed Professional Competencies and Competency Elements (knowledge, skills, etc., KKK Section 8) that the course significantly contributes to developing (highlight the most important ones).	

a) Knowledge

- Has a research-level understanding of the general and specific characteristics, major directions, and precisely developed boundaries of the subject area within the discipline, as well as the agreed and debated interrelations.
- Creatively comprehends the interrelations, theories, and conceptual frameworks and terminologies of the given field of study.¹
- Possesses research methodology knowledge necessary for independent research in the given discipline/field.

b) Skills

- Capable of creative analysis of the field, synthesizing comprehensive and specific interrelations with a new perspective, and conducting appropriate evaluative and critical activities.
- Able to apply and further develop the specialized learning and problem-solving methods of the field.
- Can creatively elaborate on the novel, previously unknown practical implications of theoretical issues.
- Capable of planning and executing new projects, conducting research in the field, and developing new techniques and approaches.
- Able to identify unforeseen professional problems and uncover the detailed theoretical and practical background necessary for their resolution at a research level.
- Can construct and communicate new relations relevant to the field, as well as comprehensive interrelations significant for personal and communal existence.

c) Attitudes

- Represents and further develops the relations that contribute to the process of human self-creation based on the field's characteristics.
- Possesses an interest and learning ability that enable identifying and solving currently unpredictable research problems in the field.
- Demonstrates a firm professional commitment, a continuous dedication to exploring new approaches, and an acceptance of the necessity for persistent effort.

d) Autonomy and Responsibility

- Builds and initiates new knowledge areas with creative independence and proposes new practical solutions.
- Participates in formulating theoretical and practical questions with a leadership role and high-level cooperation.
- Engages as an equal discussion partner with professionals in the field.
- Takes responsibility for raising and addressing new ethical questions concerning theoretical and practical aspects of the profession.

¹**Section 108**, Article 37 of the National Curriculum Act (Nftv.) 37. lesson: a session (lecture, seminar, exercise, consultation) requiring the personal involvement of the instructor to fulfil the academic requirements specified in the curriculum, the duration of which is at least forty-five minutes and not more than sixty minutes.

² e.g. case studies, role play, thematic presentations, etc.

³ e.g. continuous debriefing, mid-year report

⁴ e.g. request for case studies, thematic papers, essays, business, organisational plans, etc.

Course responsible (name, position, academic degree): **dr. Péter Ligeti, Habil. Associate Professor, PhD**

Instructor(s) involved in teaching the course (if any) (name, position, academic degree):
dr. Péter Kutas, Associate Professor, PhD.