Course name: **Applied Cryptography Project Seminar**	Credit value: **6**
Theoretical-practical division : **30-70** (credit%)	
Course time (in 45-minute classroom units) **Lecture: 26** **Practice (lab): 26** **Consultation: 26**	
Grading: exam + practice development assignments	
Recommended semester: Semester 3	
Recommended prerequisites: Basics of cryptography and security (covered e.g. in the course "Cryptography" or "Introduction to Computer Security")	

Syllabus

The purpose of the course is to help develop a prototype application that uses cryptographic protocols learnt in class. There are two main types of applications.

- The student can develop a small web-based application, mobile application or similar prototype application implementing security and privacy oriented parts of the software using methods and protocols covered in class. Examples of protoypes that could be given as assignment can include the following.
  - A set of blockchain smart contracts implementing a distributed on-chain algorithm
  - A mobile or web application implementing security and privacy features, e.g. a secure voting protocol over secure channels
  - A fork of an existing open-source project with added or modified features
- The student can focus on more research-oriented development.
  - Implementation of experimental protocols from research papers
  - Meta-analysis of studies for the comparison of various cryptographic approaches to specific problems, based on efficiency, security, cost etc. characteristics

The completion of the assignments prepares the student for the participation in larger projects involving security-critical parts.

Recommended literature

Niels Ferguson, Bruce Schneier, Tadayashi Kohno: **Cryptography Engineering: Design Principles and Practical Applications**. Wiley Publishing, 2010. ISBN: 0470474246

Gary McGraw: **Software Security Library** (Building Secure Software: How to Avoid Security Problems the Right Way, Exploiting Software: How to Break Code, Software Security: Building Security In), Addison-Wesley, 2006, ISBN: 0321418700

Jonathan Katz, Yehuda Lindell: **Introduction to Modern Cryptography.** Chapman & Hall/Crc Cryptography and Network Security Series, 2007. ISBN: 1584885513

Various further parts from the literature

Output

a) Knowledge

- They have comprehensive and up-to-date knowledge and understanding of the general theories, contexts, facts, and the related concepts of IT, particularly – depending on their chosen specialization – in the areas of program design, synthesis and verification, logical programming, programming languages, computing models, computer architectures, operating systems, computer networks, distributed systems, database management systems, information theory, code theory, and cryptography.
- They have comprehensive and up-to-date knowledge of the principles, methods, and problem solving approaches of the IT domain that contains processes for designing, developing, operating, and controlling of IT Systems, particularly – depending on their chosen specialization – in the areas of programming technology; design, construction and management of complex software systems and state-of-the-art databases; service-oriented program design; the design, construction and management of information systems; the design and development of internet tools and services; the design, development and management of database systems; the design, construction and management of distributed systems, cryptography, data security and data protection.

b) Skills and abilities

- They are able to analyse and apply new problem-solving methods and procedures related to their IT specialisation
- They are able to apply their mathematical, computer science and informatics skills in a novel way in order to solve tasks in IT research and development.
- They are able to professionally use scientific and technical information sources to obtain knowledge necessary for solving a problem, and to critically interpret and evaluate it.
- Under professional guidance, they are able to carry out scientific research on their own, and to prepare for further studies at postgraduate level.
- They are familiar with IT professional vocabulary, which enables them to express themselves at a high level, both orally and in writing, in their mother tongue and (at least) in English; i.e. they are able to participate in discussions and debates, to write reports, to work with, understand and utilize scientific and technical literature (e.g. professional books, chapters, articles etc.).

c) Attitude

- They follow professional and technological developments in their IT field.
- They are committed to critical feedback and evaluation based on self-examination.
- They are committed to lifelong learning, and are open to acquiring new IT competencies.
- They accept and make their co-workers apply the ethical principles of work and organizational culture as well as those of IT scientific research.
- They share their knowledge and consider it important to disseminate professional IT results.
- They consider it important to propagate and realise environmentally conscious behaviour and social responsibility, and they promote them with the help of information technology.
- They are committed to having quality requirements met and to analysing them with IT tools.
- They are open to proactive collaboration with IT and other professionals.
-

d) Autonomy and responsibility

- They take responsibility for their professional decisions made in their IT-related activities.
- They undertake to meet deadlines and to have deadlines met.
- They bear responsibility for their own work as well as for the work of their colleagues they work together with in a project.
- Regarding mission critical IT systems, they can be entrusted with developing and

operational responsibilities that are in accordance with their professional competencies.
Course responsible: **Burcsi, Péter, PhD, associate professor**
Others involved in teaching the course: TBD