

## COMPUTER SCIENCE, MASTER STUDY PROGRAMME

### COURSE DESCRIPTIONS

#### Course name: SELECTED TOPICS IN DISTRUBUTED COMPUTING

Number of ECTS credits: 6

**Content:**

Models for distributed computing. Algorithms for distributed environments - algorithms useful in computer networks (P2P etc.). Technologies for distributed computing: distributed memory, object oriented distributed system design, distributed dictionary, un-interruptability and time synchronization, distributed scheduling and process migration, remote function calls and method invocation, robustness, security. Distributed services and tools. Student also prepares a seminar in a form of survey paper or smaller practical project.

#### Course name: SELECTED TOPICS IN HUMAN-COMPUTER INTERACTION

Number of ECTS credits: 6

**Content:**

Classical and modern research topics in the field of human-computer interaction. Possible topics include:

- Basics of human-computer interaction
- Mental models
- User modeling
- User error in critical systems.
- Navigation (multiple displays, infinite canvas, information space).
- Tasks analysis and contextual design.
- User based evaluation of the system or product.
- 3D GUI
- Direct manipulation.
- Prticipatory practices.
- Prototyping.
- Design of menus.
- Virtual envoronments.
- Information visualisation.
- Augmented reality.

#### Course name: SELECTED TOPICS IN THEORETICAL COMPUTER SCIENCE

Number of ECTS credits: 6

**Content:**

Models of computing. Finite automata, stack machines and their properties; corresponding formal languages with their properties. Computability and undecidability. Nondeterminism and NP completeness. Samples of NP complete problems. Lower space and time bounds. Time and space complexity classes and relations among them. Student also prepares a seminar in a form of survey paper or smaller practical project.

**Course name: SELECTED TOPICS IN INFORMATION VISUALISATION**

Number of ECTS credits: 6

**Content:**

Classical and modern research topics in the field of information visualisation. Possible topics include:

- appropriate allocation of visual attributes to data variables,
- designing with color and luminance contrast,
- the psychology of human vision and perception,
- visual analytics,
- interaction,
- storytelling,
- text visual analytics,
- big data visualization,
- uncertainty visualization,
- network visualization,
- cartographic visualization,
- animation and time series visualization.

**Course name: SELECTED TOPICS IN CRYPTOGRAPHY**

Number of ECTS credits: 6

**Content:**

The modern society heavily relies on secure telecommunication and electronic commerce over the Internet. The internet also provides an easy access to various data bases. The smart cards were revolutionary cryptographic primitives with possibility of some moderate computing on a small-sized footprint. Its application area includes e.g. health care, education and is constantly expanding.

Cryptography is a science that offers us practical solutions for security and protection of the information, thus it is regarded as one of the major security mechanisms today (goals: secrecy, message integrity, electronic signatures, digital cash, and other cryptographic protocols; Field: mathematics, computer science, electrotechnics, finance, politics, military, etc. ) The course will cover the following topics:

- (A) Symmetric ciphers
  - (B) Public key cryptography
  - (C) Digital signatures
  - (D) Cryptographic protocols
  - (E) Algorithmic number theory
  - (F) Hash functions
  - (G) Algebraic attacks
- 
- (A) Symmetric ciphers
    - Stream ciphers
    - Analysis of some particular ciphers such as RC4
    - Generic attacks on block ciphers
    - Cryptanalysis of specific block ciphers e.g. AES
    - The use of block and stream ciphers
    - Pseudo-random number generators
    - Cryptanalysis of 3-DES
    - Cryptanalysis of DESX-a
    - Cryptanalysis of pseudo-random number generators
  - (B) Public key cryptography
    - RSA attacks
    - Attacks on ElGammal cryptosystems

- Pseudo-random number generators using discrete algorithms (analysis of linear and quadratic congruence generators and some weaknesses w.r.t to their use in DSA (Digital Signature Algorithm))
  - XTR (PKC of Lenstra et al.)
  - NTRU a new PKC standard
  - LUC (public key cryptosystem without using operation of exponentiation)
  - McEliece cryptosystem with Goppa codes
- (C) Digital signatures
- Blind signatures
  - Group signatures
  - One-time signatures
- (D) Various cryptographic protocols
- Digital cash
  - Anonymity
  - Shared security
  - Mental poker over the phone
  - Resilient functions
  - Kleptography (stealing information securely)
  - Key escrow ( is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys)
  - Visual cryptography (and Hadamard matrices)
  - Identification schemes
- (E) Algorithmic number theory
- Optimal computation in finite fields
  - Polynomial basis
  - Normal bases (e.g. optimal normal bases or Chebishev basis)
  - Transformation of different basis in finite fields  $GF(p^n)$
  - Integer factorization
  - Pollard's rho-method for factorization
  - Factorization of polynomials
  - Generation of prime numbers
  - Probabilistic primality tests (e.g. with elliptic curves)
  - Prime factorization is in P ?
  - Discrete log problem (DLP)
  - Pollard's rho method for DLP
  - Floyd's algorithm
- (F) Hash functions
- Description and analysis of hash functions HMAC
  - Description and analysis of hash functions RIPEMD
- (G) Attacks
- Methods using the birthday paradox (which is used in cryptanalysis of both symmetric and asymmetric cryptosystems).