Course title: Cryptography and Computer Security

Course code: 63528

ECTS: 6

Professor: Aleksandar Jurišić

Master's program

Prerequisite knowledge (please be specific if possible):

- undergraduate mathematics (CS, definition of a group, vector space, probability,...), and above all the readiness to solve problems individually and/or program some simple (cryptographic) algorithms.

Specifically, it helps if a student is already familiar with:

- elementary number theory and modular arithmetics (algorithms such as: fast calculation of powers - square-multiply, multiplicative inverse), Euler's function, Fermat's theorem, Euler's generalization
- (extended) Euclidean algorithm, Chinese remainder theorem
- algorithmic number theory (theory of computations, complexity theory, reductions and NP completeness)

(although we usually make a brief review of some of the above topics if necessary).

Short course decription (max half of the page):

Information/Computer Security describes all preventive measures, procedures and means to ensure access to Information Systems and their contents in order to prevent their unauthorized use. Cryptography provides maximum security while at the same time preserve its flexibility of digital media. It forms the foundation of Information Society (objectives: privacy, data integrity, digital authentication/signatures, digital cash, and other cryptographic protocol; in covers Mathematics, Computer Science, Electrical Engineering, Finances, Policy, Defense, etc.).

The course will cover the following topics:

Symmetric cryptography

– classical Ciphers and History of Cryptography
– Kerckhoff Principle and various attacks to cryptosystems
– Shannon Theory of Information and Entropy
(Perfect, Computational and Provable Security)
– Block Ciphers
(DES/IDEA, AES and finalists, Linear and Differential Analysis)
– Stream Ciphers/PRNG (LFSR and Berlekamp-Massey algorithem, RC4,...),
– Cryptoanalysis and Statistical Methods
– Hash Functions (MD/SHA, HMAC, ...) and Authentication Codes (MAC),

Birthday Paradox Attacks, new attacks,...

Public-key cryptography (Asymmetic Cryptography)

– Perfect Security (Computational, Unconditional and Provable Security)
– Public-Key Cryptosystems, One-Way Functions and related problems in Number Theory (Primality Testing, Integer Factorization, Discrete Logarithem Problem)
– Digital Signatures (RSA, DSA, one-time, blind, group etc.)
– Key Agreement Protocols (Diffie-Hellman, ElGamal, Kerberos, STS)
– Identification Schemes for humans and devices (challenge/response, ...)
– Other protocols (head/tail over the phone, mental poker, Secret Sharing Schemes, Authentication Schemes, Timestamps, Visual Cryptography, Zero-Knowledge Proofs)
– Quantum cryptography

Computer and information security (Do we need security in CS?)

– Security of programs (bugs, viruses, malicious code)
– Security of data bases (anonymization)
– Security of OS (MS Win, Unix/Linux, liveCD)
– Security of network communication (firewalls, VPN, IPSec, SSL)
– Privacy in CS (tokens/smart cards, RFID cards)
– Key management (certificates, CA, PKI, X.509)
– Efficient and secure implementations of cryptosystems (sidechanell attacts and defences agains them)
– Real time security management (security policy, monitoring)
– Patents and standards (ISO, IEEE, IETF)