Óbuda University John von Neumann Faculty of Informatics			Institute of Biomatics and Applied Artificial Intelligence	
Name and code: Cryptography and quantum cryptography NMXCC1EMNF **Credits:5** *2025/26 year, II. semester*				
Subject lecturers: Marta Takacs				
Prerequisites (with code):	-			
Weekly hours:4	Lecture:2	Seminar.:	Lab. hours:2	Consultation:
Way of assessment:	exam			

Course description:

Goal: The aim of the course is to familiarize students with the mathematical background required for cryptographic primitives and the algorithms related to them. The lectures will present encryption procedures that guarantee the security of cryptographic algorithms. From a practical perspective, students will learn about their implementation.

Course description: Historical overview, brief introduction to mono- and polyalphabetic systems, DES AES, divisibility, primes, number theory basics, relative prime, remainder division, linear congruence, remainder classes, first degree congruence equations, Euler's φ function, Euler's theorem, little Fermat's theorem, Wilson's prime test, Fermat's prime test, AKS prime test, algebraic structure of fields, finite fields, field extension, RSA, SSL/TLS, PGP, elliptic curves, operation with elliptic curves, elliptic curves over finite fields, Diffie-Helmann key exchange, electronic signature properties, signature logic, signature content, signature with RSA, signature with elliptic curves, algorithms of quantum cryptography, Post quantum cryptography, standardizations

Lecture schedule

Education week	*Topic*
1.	Historical overview, motivation, Basic concepts, Classical and modern encryption methods, practical examples of use: digital signature, message seal, key management, cryptography in communication
2.	Symmetric key encryptions (DES, AES)
3.	Fundamentals of number theory
4.	Congruence relations, congruence equations, prime tests
5.	Congruence relations, congruence equations, prime tests
6.	Operations over finite fields, field expansion
7.	Asymmetric key encryptions (RSA)
8.	Security protocols (SSL/TLS, PGP)
9.	Elliptic curves
10.	Electronic signature
11.	Algorithms of quantum informatics and quantum cryptography
12.	Post-quantum cryptography, Limits of quantum cryptography
13.	Midterm exam
14.	Retake of midterm exam

Midterm requirements

Conditions for obtaining a signature:
- uploading the homework assignments given during the lectures to the Moodle system (can be counted as 50% towards the exam grade)
- writing the midterm exam with at least a satisfactory grade (can be counted as a maximum of 50% towards the exam grade).

Final grade calculation methods

The final grade is calculated as follows:
Midterm exam: 50 points, individual project, uploaded homework at best 50 points.
Final exam in the exam period is mandatory if the offered grade based on the cumulative result during the semester activity is not acceptable for the student or the cumulative points are below 50 points.

Achieved result	Grade
89%-100%	excellent (5)
76%-88<%	good (4)
63%-75<%	average (3)
51%-62<%	satisfactory (2)
0%-50<%	failed (1)

Type of exam

Oral/written answer from the theoretical background. (at best 50 points, 50% of the whole result).

Type of replacement

At the last week of the semester period the student has possibility to present his missed individual home works and mid-term exam (replacement).
A student who has written the midterm exam and submitted homework, but has not achieved the 30% requirement is eligible for a signature replacement at the first week of the exam period. A student who has not appeared for the midterm exam or its replacement, has not submitted homework or project assignments, or has been absent from more than half of the classes without justification is not eligible for a signature replacement.

References

Obligatory:
recommended slide series from classes, by subjects, available on the Moodle system

Recommended:
Zhiyong Zheng: Modern Cryptography Volume 1: A Classical Introduction
Springer; 1st ed. 2022 edition (2022); eBook (Creative Commons Licensed), **ISBN-10:** 9811909229, **ISBN-13:** 978-9811909221
Zhiyong Zheng , Kun Tian , Fengxia Liu: Modern Cryptography Volume 2: Post-Quantum Cryptography, Springer; 1st ed. (2023), **ISBN-10:** 9811976465, **ISBN-13:** 978-9811976469