Subject (course) name: **APPLIED CRYPTOGRAPHY**		
Programme: **Computer Science** Specialty:		Subject code: **15**
		Title graduate: **Engineer**
Type of course: **obligatory**	Course level: **First-cycle studies**	Year: **III** Semester: V**I** Semester: **summer**
Form of classes: **Lectures, Classes, Labs, Seminar, Project**	Number of hours per week: **1L, 0, 2Lab, 0, 0**	Credit points: **5 ECTS**

GUIDE TO SUBJECT

SUBJECT OBJECTIVES

C1. Supplying the necessary knowledge of the mathematical foundations of cryptography.

C2. Learning basic symmetric ciphers.

C3. Learning algorithms of public key.

C4. Learning basic digital signature algorithms.

C5. Acquisition by students the methods of separation of confidential information.

SUBJECT REQUIREMENTS

1. Discrete Mathematics.
2. Linear Algebra.
3. Mathematical Analysis.

LEARNING OUTCOMES

EK 1 – The Student is able to calculate and to interpret the following quantities characterizing the ciphertext: entropy, the language indicator, redundancy, conditional entropy and critical length. The Student is able to evaluate the safety algorithm based on its computational complexity. The Student is fluent in modular arithmetics and knows the rules to generate prime numbers.

EK 2 – The Student knows the DES algorithm and is able to present its block diagram. The Student is able to demonstrate examples of this encryption algorithm.

EK 3 – The Student knows the RSA algorithm and is able to present the principles of operation and examples of encryption.

EK 4 – The Student knows the DSA digital signature algorithm. Student is able to provide complete examples of the signature creation algorithm.

EK 5 – The Student knows the protocol sharing principles between 2 agents and information

sharing protocol between N agents. Student is able to create a diagram of a threshold secret sharing method a) with the Lagrange interpolation algorithm and b) with using the "shadow information". The Student knows exchange and management key protocols.

SUBJECT CONTENT

Form of classes - lectures

Topic	Hours
W 1 – Fundamentals of information theory, computational complexity of the algorithm, modular arithmetics.	**2**
W 2 – Substitution ciphers, ciphers with one alphabet, ciphers with N alphabets..	**1**
W 3 – Ciphering rotor machine – ENIGMA.	**1**
W 4 –Exponential encryption basis. DES algorithm.	**2**
W 5 – Public key algorithms: RSA algorithm.	**2**
W 6 – Hash functions.	**1**
W 7 – Digital signature algorithms: DSA digital signatures algorithm.	**2**
W 8 – Cryptographic protocols. Detection of protocol violations. Transmission and exchange information protocols. Key management protocols.	**2**
W 9 – Cryptography in databases.	**2**
Total	**15**

Form of classes – laboratory

Topic	Hours
L 1 – Prime numbers: the first number generator, Sieve of Eratosthenes. Coprime integers: Euclidean algorithm, Euler function. The exponent inverting in the set of natural numbers.	**4**
L 2 – Preparation of the text to encrypt: the division of text on signs.	**2**
L 3 – Ciphers: permutation cipher.	**2**
L 4 - Ciphers: Cezar cipher.	**2**
L 5 – Ciphers: Playfair cipher.	**4**
L 6 – Ciphers: Vigenere cipher.	**4**
L 7 – The RSA cryptosystem.	**2**
L 8 - The Hill cryptosystem.	**2**
L 9 – Asymmetric Digital Signature - Generate a signature using RSA cipher.	**2**
L 10 – Diffie-Hellman key agreement system.	**2**
L 11 – Information sharing protocol between n agents.	**4**
Total	**30**

STUDY METHODS

1. Lectures using multimedia presentations.
2. Laboratory - working alone and in groups.

EDUCATIONAL TOOLS

1. Audio and visual equipment.
2. Computer laboratory.

METHODS OF ASSESMENT (F – Forming, P – Summary)

F1. Assessment of preparation for classes – oral answer.
F2. Assessment of the correctness and timeliness of presentation software created.
P1. Lecture – written exam.
P2. Laboratory – tests.

STUDENT WORKLOAD

Form of activity	Averaged workload (hours)		
	[h]	∑ [h]	ECTS
Participation in class activities lecture laboratory	15 30	45	3
Preparation for tutorials (reading literature)	15	35	2
Preparation for laboratory	20		
Total		**80**	**5**

A. BASIC READING

1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, **Handbook of Applied Cryptography, INTERNET ARCHIVE**
2. Richard E. Klima, Neil Sigmon, Ernest Stitzinger, Applications of Abstract Algebra with MAPLE, CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 1999.
3. Peter M. Higgins, Number Story, From Counting to Cryptography, COPERNICUS BOOKS, An Imprint of Springer Science+Business Media, © Springer-Verlag London Limited 2008.

B. FURTHER READING

1. Song Y.Yan, Number Theory for Computing, Second Edition, Springer-Verlag, Berlin, Heilderberg 2002
2. Victor Shoup, A Computational Introduction to Number Theory and Algebra, Copyright _c 2005 by Victor Shoup, <victor@shoup.net>

Learning objectives	In relation to the learning outcomes specified for the field of study	Subject objectives	Subject content	Course study methods	Methods of assessment	Learning objectives
EK1	K_W05	T1A_W03 T1A_W04	C1	lecture laboratory	**1,2**	P1/P2
EK2	K_W05	T1A_W03 T1A_W04	C2	lecture laboratory	**1,2**	P1/P2
EK3	K_W05	T1A_W03 T1A_W04	C3	lecture laboratory	**1,2**	P1/P2
EK4	K_W05	T1A_W03 T1A_W04	C4	lecture laboratory	**1,2**	P1/P2
EK5	K_W05, K_U12	T1A_W03 T1A_W04 T1A_U14 T1A_U15 T1A_U16 InzA_U07	C8	lecture laboratory	**1,2**	P1/P2

II. EVALUATION

Grade	Outcome
EK1	
2	The Student cannot calculate and interpret the following quantities: entropy, language signature and critical length. The Student does not know the foundations of modular arithmetics and student does not know the methods for generating the

	primary numbers.
3	The Student can calculate and interpret the following quantities: entropy, language signature and critical length. The Student knows the basic modular arithmetics, and the methods for generating the primary numbers.
4	The Student can calculate and interpret the following quantities: entropy, language signature, redundancy, conditional entropy, critical length. The Student knows definition of computational complexity of an algorithm. The Student knows the basic modular arithmetics, and the methods for generating the primary numbers.
5	The Student can calculate and interpret the following quantities: entropy, language signature, redundancy, conditional entropy, critical length. The Student can estimate computational complexity of the algorithm and he can estimate its secure level. The Student knows the basic modular arithmetics, and the methods for generating the primary numbers.
EK2	
2	The Student does not know DES algorithm and He/She can't present its block scheme and He/She can't present any example of coding with the DES algorithm.
3	The Student knows DES algorithm.
4	The Student knows DES algorithm and He/She can present its block scheme.
5	The Student knows DES algorithm and He/She can present its block scheme and He/She can present an example of coding with the DES algorithm.
EK3	
2	The Student does not know RSA algorithm and He/She can't present its block scheme and He/She can't present any example of coding with the RSA algorithm.
3	The Student knows RSA algorithm.
4	The Student knows RSA algorithm and He/She can present its block scheme.
5	The Student knows RSA algorithm and He/She can present its block scheme and He/She can present an example of coding with the RSA algorithm.
EK4	
2	The Student doesn't know the DSA digital signature algorithm and He/She is not able to provide complete examples of the signature creation algorithm.
3	The Student knows the DSA digital signature algorithm.
4	The Student knows the DSA digital signature algorithm and He/She is able to provide complete examples of the signature creation algorithm
5	The Student knows the DSA digital signature algorithm and He/She is able to provide complete examples of the signature creation algorithm. The Student is able to modify algorithm DSA.
EK5	
2	The Student does not know the protocol information sharing between 2 agents and information sharing protocol between N agents.
3	The Student knows the protocol information sharing between 2 agents and information sharing protocol between N agents.
4	The Student knows the protocol information sharing between 2 agents and information sharing protocol between N agents. The Student is able to create a diagram of a threshold secret sharing method, both a) Lagrange interpolation algorithm and b) using the "shadow information".

5	The Student knows the protocol information sharing between 2 agents and information sharing protocol between N agents. The Student is able to create a diagram of a threshold secret sharing method, both a) Lagrange interpolation algorithm and b) using the "shadow information". The Student knows exchange and management key protocols.

III. OTHER USEFUL INFORMATION

1. All information for students on the schedule are available on the notice board and on the website: www.el.pcz.czest.pl
2. Information on the consultation shall be provided to students during the first lecture and will be placed on the website www.el.pcz.czest.pl
3. Terms and conditions of credit courses will be provided to students during the first lecture