Course Syllabus

I. General Information

Course name	Data protection
Programme	Informatics
Level of studies (BA, BSc, MA, MSc, long-cycle MA)	BA
Form of studies (full-time, part-time)	full-time
Discipline	Informatics
Language of instruction	English

Course coordinator	dr Viktor Melnyk prof. KUL

Type of class *(use only the types mentioned below)*	Number of teaching hours	Semester	ECTS Points
lecture	30	III	5
tutorial			
classes			
laboratory classes	30	III	
workshops			
seminar			
introductory seminar			
foreign language classes			
practical placement			
field work			
diploma laboratory			
translation classes			
study visit			

Course pre-requisites	PR_1 - knowledge of informatics covered by the high school program. PR_2 - basic knowledge of discreet and modular arithmetic. PR_3 - good computer skills.

II. Course Objectives

C_1 - to familiarize students with the up-to-date principles, techniques, and algorithms of interest in cryptographic practice with emphasis placed on those aspects which are most practical and applied.
C_2 - to present specific security solutions used in modern computer and telecommunication systems and networks.

III. Course learning outcomes with reference to programme learning outcomes

Symbol	Description of course learning outcome	Reference to programme learning outcome
KNOWLEDGE		
W_01	Theoretical knowledge of information security goals, principles and application aspects	K_W04, K_W06
W_02	Theoretical knowledge of cryptographic primitives and algorithms to provide basic security goals	K_W03, K_W04, K_W06
W_03	The student knows the principles of operation of symmetric encryption algorithms, both stream and block ciphers	K_W03, K_W04, K_W06, K_W10
W_04	The student knows the principles of operation of asymmetric encryption algorithms	K_W03, K_W04, K_W06, K_W10
W_05	The student knows the principles of operation hashing algorithms and functions	K_W03, K_W04, K_W06, K_W10
W_06	The student has knowledge of the digital signature algorithms. The student understands and can estimate the characteristics of cryptographic algorithms implementation in both software and hardware.	K_W03, K_W04, K_W06
SKILLS		
U_01	Ability to use specific technical measures to manage risks when processing personal data like: encryption, secure digital storage, back up data, secure digital communications, secure physical environment, secure disposal of data.	K_U02
U_02	Ability to carry out risk analysis and threat modelling	K_U02
U_03	Ability to apply models and guidelines for development of secure software applications	K_U02
U_04	Ability to identify and use APIs for encryption and authentication for web applications	K_U02
SOCIAL COMPETENCIES		
K_01	Skillfully solve complex problems with which they can meet in life, using the known data protection principles, objectively assessing the results	K_K01, K_K05
K_02	Follow ethical standards applicable in the IT industry.	K_K05
K_03	Work efficiently, in teams and individually, skillfully assessing priorities in the implementation of the project	K_K01, K_K05

IV. Course Content

LECTURES
1. Introduction to Cryptography and Data Security
2. Symmetric Cryptography
3. Stream Ciphers
4. Block Ciphers
5. Public-Key Cryptography
6. The RSA Cryptosystem
7. Elliptic Curve Cryptosystems
8. Digital Signatures
9. Hash Functions
10. Message Authentication Codes

11. Key Establishment

CLASSES
1. Monoalphabetic replacement cipher (Caesar's cipher)
2. Permutation cipher
3. Cryptanalysis of monoalphabetic replacement ciphers
4. Organization of a steganographic channel in a BMP file
5. Symmetric block ciphers based on the Feistel network
6. Modern computerized methods of encrypting and decrypting text messages
7. Data encryption using the AES algorithm

V. Didactic methods used and forms of assessment of learning outcomes

Symbol	Didactic methods *(choose from the list)*	Forms of assessment *(choose from the list)*	Documentation type *(choose from the list)*
KNOWLEDGE			
W_01 W_02	Conventional lecture	Exam / Written test	Evaluated test / written test
W_03 W_04 W_05 W_06	Conventional lecture, Laboratory classes	Exam / Written test, Test of practical skills, Observation	Evaluated test / written test, Rating card / Observation report, Protocol / report printout/ report file
SKILLS			
U_01 U_04	Laboratory classes, Practical classes design thinking	Test of practical skills, Observation	Rating card / Observation report Protocol / report printout/ report file
SOCIAL COMPETENCIES			
K_01 K_02	Conventional lecture, Laboratory classes design thinking	Exam / Written test, Test of practical skills, Observation	Evaluated test / written test, Rating card / Observation report, Protocol / report printout/ report file
K_03	Laboratory classes design thinking	Test of practical skills, Observation	Rating card / Observation report, Protocol / report printout/ report file

VI. Grading criteria, weighting factors…

The final assessment (for those who passed the classes) consists in conducting a test of the knowledge provided during the lectures. The exam grade is formed on the basis of two components:

70 % - written answers to test tasks and oral answers in case of doubt,
30% - the grade obtained from the classes.

A grading scale is given below:

90 – 100% - very good (5.0),
80 – 89% - good plus (4.5),
70 – 79% - good (4.0),
60 – 69% - satisfactory plus (3.5),

50 – 59% - satisfactory (3.0),
Less than 50% - unsatisfactory (2.0).
Detailed assessment rules are given to students with each subject edition.

VII. Student workload

Form of activity	Number of hours
Number of contact hours (with the teacher)	**60**
Number of hours of individual student work	**60**

VIII. Literature

Basic literature
1. Understanding Cryptography: A Textbook for Students and Practitioners, 1st ed. 2010 Edition, by Christof Paar, Jan Pelzl. Springer, 2010. 2. Stallings, W. Cryptography and Network Security: Principles and Practice (6th Edition). USA: Pearson, 2013. 3. Menezes A., Oorshot P., Vanstone S. Handbook of applied cryptography. – N.Y.: CRC Press Inc., 1996. – 816 p. 4. Understanding Privacy and Data Protection: What You Need to Know by Timothy J. Toohey, 2014. 5. Modern Cryptography: the Basic Terms. V. Emets, A. Melnyk, R. Popovych. Lviv, BAK, 2003. 144p.
Additional literature
1. T. Korkishko, A. Melnyk, V. Melnyk. „Algorithms and Processors of Symmetric Block Encryption. Series: Information Protection in Computer and Telecommunication Networks ". Lviv, BAK, 2003, - 169 pp. 2. Daemen J., Rijmen V. AES Proposal: Rijndael // First Advanced Encryption Standard(AES) Conference. – Ventura, CA, 1998. 3. FIPS 46, "Data Encryption Standard", Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C. 4. American Bankers Association, Tripple Data Encryption Algorithm Modes of Operation, ANSI X9.52-1998, Washington, D.C., 1998. 5. FIPS 81, "Operational modes of DES", Federal Information Processing Standard (FIPS), Publication 81, National Bureau of Standards, U.S. Department of Commerce, Washington D.C. 6. S. Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor, 2000. 7. D. Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. 2nd edition, Scribner, 1996. 8. Cryptool, http://www.cryptool.de