KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	**Ochrona danych**
Nazwa przedmiotu w języku angielskim	**Data protection**
Kierunek studiów	**Informatyka w j. angielskim**
Poziom studiów (I, II, jednolite magisterskie)	**I**
Forma studiów (stacjonarne, niestacjonarne)	**stacjonarne**
Dyscyplina	**Informatyka**
Język wykładowy	**angielski**

Koordynator przedmiotu/osoba odpowiedzialna	**dr Viktor Melnyk prof. KUL**

Forma zajęć *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład	30	3	5
konwersatorium			
ćwiczenia			
laboratorium	30	3	
warsztaty			
seminarium			
proseminarium			
lektorat			
praktyki			
zajęcia terenowe			
pracownia dyplomowa			
translatorium			
wizyta studyjna			

Wymagania wstępne	W1 - knowledge of informatics covered by the high school program. W2 - basic knowledge of discreet and modular arithmetic. W3 - good computer skills.

II. Cele kształcenia dla przedmiotu

C1 - 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.
C2 - to present specific security solutions used in modern computer and telecommunication systems and networks.

III. Efekty uczenia się dla przedmiotu wraz z odniesieniem do efektów kierunkowych

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Theoretical knowledge of information security goals, principles and application aspects	K_W01 K_W02 K_W07 K_W09
W_02	Theoretical knowledge of cryptographic primitives and algorithms to provide basic security goals	K_W01 K_W02 K_W07 K_W09
W_03	The student knows the principles of operation of symmetric encryption algorithms, both stream and block ciphers	K_W01 K_W02 K_W07 K_W09
W_04	The student knows the principles of operation of asymmetric encryption algorithms	K_W01 K_W02 K_W07 K_W09
W_05	The student knows the principles of operation hashing algorithms and functions	K_W01 K_W02 K_W07 K_W09
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_W01 K_W02 K_W07 K_W09
UMIEJĘTNOŚCI		
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_U01 K_U02 K_U03 K_U04 K_U05 K_U19
U_02	Ability to carry out risk analysis and threat modelling	K_U01 K_U02 K_U04 K_U05
U_03	Ability to apply models and guidelines for development of secure software applications	K_U01 K_U02
U_04	Ability to identify and use APIs for encryption and authentication for web applications	K_U04 K_U05 K_U19
KOMPETENCJE SPOŁECZNE		
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_K03 K_K04 K_K08 K_K10
K_02	Follow ethical standards applicable in the IT industry.	K_K06 K_K07
K_03	Work efficiently, in teams and individually, skillfully assessing priorities in the implementation of the project	K_K02 K_K03 K_K04 K_K05 K_K08

IV. Opis przedmiotu/ treści programowe

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

V. Metody realizacji i weryfikacji efektów uczenia się

Symbol efektu	Metody dydaktyczne *(lista wyboru)*	Metody weryfikacji *(lista wyboru)*	Sposoby dokumentacji *(lista wyboru)*
WIEDZA			
W_01, W_02	Conventional lecture	Exam / Written test	Evaluated test / written test
W_03, W_04, W_05, W_06	Conventional lecture,	Exam / Written test, Test of practical skills,	Evaluated test / written test, Rating card / Protocol / report printout/ report file
UMIEJĘTNOŚCI			
U_01 - U_04	Laboratory classes, Practical classes	Test of practical skills,	Rating card Protocol / report printout/ report file
KOMPETENCJE SPOŁECZNE			
K_01, K_02	Laboratory classes	Exam / Written test, Test of practical skills,	Evaluated test / written test, Rating card / Protocol / report printout/ report file
K_03	Laboratory classes	Test of practical skills,	Rating card Protocol / report printout/ report file

VI. Kryteria oceny, wagi…

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. Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	**90**
Liczba godzin indywidualnej pracy studenta	**60**

VIII. Literatura

Literatura podstawowa
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.
Literatura uzupełniająca
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