Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

Name of the course in polish	:	**Zastosowania Metod Stochastycznych dla Bezpieczeństwa i Ochrony Prywatności**
Name of the course in english	:	**Applied Stochastics with Applications for Security and Privacy**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	W04INA-SM4103G
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	30			
The total number of hours of student workload (CNPS)	60	120			
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	3	3			
including the number of points corresponding to the classes of practical (P)		3			
including the number of points corresponding occupations requiring direct contact (BK)	2	2			

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

background in probability theory

COURSE OBJECTIVES

C1 presentation of techniques originating from probability theory and stochastic processes for applications in computer security technologies

C2 skills in using advanced techniques for computer security

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 posesses knowledge of discrete stochastic processes and their convergence

W2 understands threats and protection mechanisms agaist traffic analysis

W3 knows theoretical background of systems based on random processes

W4 knows self-stabilization and self-organization techniques

W5 understands the mechanisms of infection in distributed systems

W6 understands randomized algorithms used for generating and distribution of cryptographic data

The student skills:

U1 can analyze performance of a stochastic process

U2 can design and analyze solutions for defense against traffic analysis

U3 can apply random systems for construction of computer applications

U4 can design systems based on self-* paradigm

U5 can analyze processes in IT systems based on branching processes

The student's social competence:

K1 has skills for creating an abstract mathematical model for situations occuiring in practicein

COURSE CONTENT

Type of classes - lectures		
Wy1	Stochastic processes, Markov chains	4h
Wy2	Rapid mixing of Markov chains	4h
Wy3	Anonymous communication protocols, mix nets	4h
Wy4	Analysis of anonymity of Bitcoin transactions	4h
Wy5	Statistical tests	4h
Wy6	Security of pseudorandom generators and stream ciphers	4h
Wy7	Anomaly detection in systems	4h
Wy8	Risk-limiting audits	2h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Stochastic processes, Markov chains	4h
Ćw2	Rapid mixing of Markov chains	4h
Ćw3	Anonymous communication protocols, mix nets	2h
Ćw4	Random graphs and random walks	4h
Ćw5	Security systems based on random walk paradigm	2h
Ćw6	Self-stabilizing and self-organizing systems	2h
Ćw7	Branching processes, percolation and virus propagation	2h
Ćw8	Statistical tests. Anomaly detection	10h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Creating programming projects
6. Creating multimedia presentations by students
7. Consultation
8. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W6, K1-K1	Project
F2	U1-U5, K1-K1	Home assignments
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. Introduction to Probability. C. M. Grinstead, J. L. Snell
2. Probability and Random Processes. G. R. Grimmett and D. R. Stirzaker, ISBN: 0198534485
3. Random Graphs. Svante Janson, Tomasz Luczak, Andrzej Rucinski. ISBN: 0471175412
4. Markov Chains and Mixing Times. David A. Levin, Yuval Peres and Elizabeth L. Wilmer, ISBN: 0821847392
5. Finite Markov Chains and Algorithmic Applications - O. Haggstrom
6. A Gentle Introduction to Risk-limiting Audits - Mark Lindeman and Philip B. Stark

SUPERVISOR OF COURSE

dr Filip Zagórski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Zastosowania Metod Stochastycznych dla Bezpieczeństwa i Ochrony Prywatności
WITH LEARNING OUTCOMES IN THE FIELD OF ALGORITHMIC COMPUTER SCIENCE

Subject learning effect	Relating the subject effect to the learning outcomes defined for the field of study	Objectives of the course**	Program content**	Teaching tool number**
W1	K2_W01 K2_W02 K2_W05	C1	Wy1-Wy8	1 2 7 8
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W3	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W4	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W5	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W6	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
U1	K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10 K2_U12	C2	Ćw1-Ćw8	3 4 5 6 7 8
U2	K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U10	C2	Ćw1-Ćw8	3 4 5 6 7 8
U3	K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10	C2	Ćw1-Ćw8	3 4 5 6 7 8
U4	K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10	C2	Ćw1-Ćw8	3 4 5 6 7 8
U5	K2_U01 K2_U02 K2_U03 K2_U04 K2_U06 K2_U08 K2_U10 K2_U12	C2	Ćw1-Ćw8	3 4 5 6 7 8
K1	K2_K02 K2_K03 K2_K05 K2_K06 K2_K07 K2_K10 K2_K12	C1 C2	Wy1-Wy8 Ćw1-Ćw8	1 2 3 4 5 6 7 8