COURSE SYLLABUS AND SPECIFICATION

Curriculum title: **USSPR-M-O-I-S-21/22Z-MK**	
Course title: **cryptography (kryptografia) (SPECJALNOŚCI / SPECJALIZACJE / MODUŁY SPECJALNOŚCIOWE)**	Course code: **SPR17AIJ3444_110S**
Name of field of study: **matematyka**	
Mode and cycle of study: **first-degree, full - time**	Profile of study: **general academic** / Specialty: **matematyka komputerowa**
Course / module status **obligatory**	Language of instruction: **semester: 6 - english language**

Year	Semester	Form of instruction	No. of hours	w tym e-learning	Type of credit	ECTS
3	6	konwersatorium	30	0	pg	4
Total			**30**			**4**

Course / module coordinator	**prof. dr hab. FRANZ-VIKTOR KUHLMANN**
Course instructor	**dr hab. KATARZYNA KUHLMANN**
Course / module objectives	**Provide knowledge of the main principles of symmetric and asymmetric cryptosystems and some of the main encryption systems and their mathematical foundations**
Prerequisites	**Basic knowledge of arithmetic and prime numbers.**

LEARNING OUTCOMES

Category	No.	Code	Description	Ref. to programme benchmarks
knowledge	**1**	**EP1**	**The student has deepened knowledge of the most important cryptosystems and their mathematical foundations, as well as the possible attacks on these systems.**	**SMK_W01**
	2	**EP2**	**The student understands the recent developments and challenges in cryptography.**	**SMK_W01**
skills	**1**	**EP3**	**The student is able to apply the cryptosystems and to prove their properties.**	**SMK_U01**
social competences	**1**	**EP4**	**The student is ready to find necessary information in the literature, also in foreign languages.**	**SMK_K02**
	2	**EP6**	**The student understands the need for further research in cryptography.**	**SMK_K02**

CONTENT	Semester	No. of hours	w tym e-learning
Subject title: **cryptography (kryptografia)**			
Format of instruction: **konwersatorium**			
1. **Background from number theory**	6	5	0
2. **Symmetric Cryptosystems**	6	1	0
3. **AES**	6	3	0
4. **Asymmetric Cryptosystems**	6	1	0
5. **Primality Testing**	6	3	0
6. **RSA and Rabin encryption**	6	5	0
7. **Discrete Logarithm Cryptographic Schemes**	6	1	0

8. **Diffie-Hellman key exchange**	6	1	0
9. **ElGamal**	6	3	0
10. **Elliptic curve cryptography**	6	3	0
11. **Hash Functions and applications**	6	3	0
12. **Security Questions and Attacks**	6	1	0

Modes of delivery	**Lecture with discussion.**	
Assessment methods		No. of learning outcome from the syllabus
	SPRAWDZIAN	**EP1,EP2,EP3,EP6**
	ZAJĘCIA PRAKTYCZNE (WERYFIKACJA POPRZEZ OBSERWACJĘ)	**EP1,EP2,EP3,EP4,EP6**
	Metody i formy weryfikacji efektów uczenia się mogą zostać zmienione dla studentów ze szczególnymi potrzebami na warunkach i zasadach określonych w Regulaminie Studiów Uniwersytetu Szczecińskiego.	
Grading criteria	**To pass the course the student needs to pass the test.**	
	Grade calculation principles	
	The final grade is the one obtained on the seminar.	

Final grade calculation method	Sem.	Course	Type of credit	Grade calc. method	Weight for the average
	6	cryptography (kryptografia)		Nieobliczana	
	6	cryptography (kryptografia) [konwersatorium]	zaliczenie z oceną		

Basic reading	J. A. Buchmann (2004): Introduction to Cryptography. Undergraduate Texts in Mathematics, Springer
Supplementary reading	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996): Handbook of Applied Cryptography, CRC Press
	C. Vanden Eynden (2001): Elementary Number Theory, McGraw-Hill
	Neal Koblitz (1994): A course in number theory and cryptography, Springer GTM 114

STUDENT WORKLOAD

	No. of hours	
		W tym e-learning
Contact hours	**30**	**0**
Participation in test / exam	**4**	**0**
Preparation for contact hours	**20**	**0**
Private reading and studying	**20**	**0**
Participation in tutorials	**16**	**0**
Preparation of project / essay / etc.	**0**	**0**
Preparation for test / exam	**10**	**0**
TOTAL workload	**100**	
ECTS credits	**4**	

COURSE SYLLABUS AND SPECIFICATION

Curriculum title: **USSPR-M-O-I-S-22/23Z**	
Unit: **Przedmiot do wyboru [moduł]**	
Course title: **analytical geometry (geometria analityczna) (PODSTAWOWE)**	Course code: **SPR17AIJ3444_2S**
Name of field of study: **matematyka**	
Mode and cycle of study: **first-degree, full - time**	Profile of study: **general academic** / Specialty:
Course / module status **elective**	Language of instruction: **semester: 3 - english language**

Year	Semester	Form of instruction	No. of hours	w tym e-learning	Type of credit	ECTS
2	3	konwersatorium	30	0	pg	4
		lecture	30	0	pg	
Total			**60**			**4**

Course / module coordinator	**dr DAWID KĘDZIERSKI**
Course instructor	**dr hab. KATARZYNA KUHLMANN**
Course / module objectives	**The aim of the subject is to develop the ability to freely use basic concepts and tools of bilinear algebra and analytical geometry over finite dimensional spaces.**
Prerequisites	**Knowledge of the basic concepts and tools of linear algebra.**

LEARNING OUTCOMES

Category	No.	Code	Description	Ref. to programme benchmarks
knowledge	**1**	**EP1**	**Student knows basic concepts and facts of linear algebra and analytic geometry.**	**K_W03 K_W04 K_W09**
	2	**EP3**	**Student is able to use determinants for recognition of Euclidean spaces**	**K_W01 K_W12**
skills	**1**	**EP2**	**Student is able to recognize the structure of affine space and its subspace.**	**K_U01 K_U12**
	2	**EP4**	**Student is able to diagonalize orthogonal matrices and can classify hypersurfaces of degree 2.**	**K_U01 K_U14**
social competences	**1**	**EP5**	**Student knows limitations of his own knowledge and understands the need for further education**	**K_K01**

CONTENT	Semester	No. of hours	w tym e-learning
Subject title: **analytical geometry (geometria analityczna)**			
Format of instruction: **lecture**			
1. **Bilinear and quadratic forms, matrix of bilinear form, orthogonal spaces, perpendicular bases and orthogonalization methods, Euclidean spaces, Sylvesters theorem, isomorphisms of bilinear spaces.**	3	6	0
2. **Affine spaces, subspaces of affine spaces, point bases, affine coordinate systems.**	3	6	0
3. **Affine maps and their relationship with linear maps.**	3	6	0
4. **Linear and affine Euclidean spaces, Euclidean norm and metric, angles and their measures, linear and affine isometries, classification of plane isometres, Grams matrix and determinant.**	3	6	0
5. **Hypersurfaces of grade 2: canonical forms, classification of curves and hypersurface of grade 2.**	3	6	0

Format of instruction: **konwersatorium**			
1. **Bilinear and quadratic forms, matrix of bilinear form, orthogonal spaces, perpendicular bases and orthogonalization methods, Euclidean spaces, Sylvesters theorem, isomorphisms of bilinear spaces..**	3	9	0
2. **Affine spaces, subspaces of affine spaces, point bases, affine coordinate systems.**	3	6	0
3. **Affine maps and their relationship with linear maps.**	3	6	0
4. **Linear and affine Euclidean spaces, Euclidean norm and metric, angles and their measures, linear and affine isometries, classification of plane isometres, Grams matrix and determinant.**	3	9	0

Modes of delivery	**subject exercises,, problem discussion, seminar lecture, information lecture,**	
Assessment methods		No. of learning outcome from the syllabus
	KOLOKWIUM	**EP1,EP2,EP3,EP4,EP5**
	ZAJĘCIA PRAKTYCZNE (WERYFIKACJA POPRZEZ OBSERWACJĘ)	**EP1,EP2,EP3,EP4,EP5**
	Metody i formy weryfikacji efektów uczenia się mogą zostać zmienione dla studentów ze szczególnymi potrzebami na warunkach i zasadach określonych w Regulaminie Studiów Uniwersytetu Szczecińskiego.	
Grading criteria	**The final grade is a summary assessment of points from activity (presentation of homework, maximum 50%) and a written test (50%).**	
	Grade calculation principles	
	The final grade is the arithmetic mean of grades from both forms of classes.	

Final grade calculation method	Sem.	Course	Type of credit	Grade calc. method	Weight for the average
	3	analytical geometry (geometria analityczna)		Arytmetyczna	
	3	analytical geometry (geometria analityczna) [konwersatorium]	zaliczenie z oceną		
	3	analytical geometry (geometria analityczna) [wykład]	zaliczenie z oceną		

Basic reading	Igor R. ShafarevichAlexey O. Remizov (2013): Linear Algebra and Geometry, Springer, Berlin, Heidelberg
Supplementary reading	Giovanni Landi, Alessandro Zampini (2018): Linear Algebra and Analytic Geometry for Physical Sciences, Springer;

STUDENT WORKLOAD

	No. of hours	
		W tym e-learning
Contact hours	**60**	**0**
Participation in test / exam	**4**	**0**
Preparation for contact hours	**10**	**0**
Private reading and studying	**5**	**0**
Participation in tutorials	**11**	**0**
Preparation of project / essay / etc.	**0**	**0**
Preparation for test / exam	**10**	**0**
TOTAL workload	**100**	
ECTS credits	**4**	