S Y L A B U S (KARTA PRZEDMIOTU)

Nazwa programu studiów: **USSPR-M-O-I-S-21/22Z-MK**	
Nazwa przedmiotu: **cryptography (kryptografia)** **(SPECJALNOŚCI / SPECJALIZACJE / MODUŁY SPECJALNOŚCIOWE)**	Kod przedmiotu: **SPR17AIJ3444_110S**
Nazwa kierunku: **matematyka**	

Forma studiów: **I stopnia lic., stacjonarne**	Profil studiów: **ogólnoakademicki**	Specjalność: **matematyka komputerowa**
Status przedmiotu: **obowiązkowy**	Język przedmiotu: **semestr: 6 - język angielski**	

Rok	Semestr	Forma zajęć	Liczba godzin		Forma zaliczenia	ECTS
				w tym e-learning		
3	6	konwersatorium	30	0	ZO	4
Razem			**30**			**4**

Koordynator przedmiotu:	**prof. dr hab. FRANZ-VIKTOR KUHLMANN**
Prowadzący zajęcia:	**dr hab. KATARZYNA KUHLMANN**
Cele przedmiotu:	**Provide knowledge of the main principles of symmetric and asymmetric cryptosystems and some of the main encryption systems and their mathematical foundations**
Wymagania wstępne:	**Basic knowledge of arithmetic and prime numbers.**

EFEKTY UCZENIA SIĘ

Kategoria	Lp	KOD	Opis efektu	Odniesienie do efektów dla programu
wiedza	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**
umiejętności	1	EP3	**The student is able to apply the cryptosystems and to prove their properties.**	**SMK_U01**
kompetencje społeczne	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**

TREŚCI PROGRAMOWE ZAJĘĆ I KONSULTACJI	Semestr	Liczba godzin zajęć	
			w tym e-learning
Przedmiot: **cryptography (kryptografia)**			
Forma zajęć: **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

Metody kształcenia	**Lecture with discussion.**	
Metody weryfikacji efektów uczenia się		Nr efektu uczenia się z sylabusa
	SPRAWDZIAN	**EP1,EP2,EP3,EP6**
	ZAJĘCIA PRAKTYCZNE (WERYFIKACJA POPRZEZ OBSERWACJĘ)	**EP1,EP2,EP3,EP4,EP6**
Forma i warunki zaliczenia	**To pass the course the student needs to pass the test.**	
	Zasady wyliczania oceny z przedmiotu	
	The final grade is the one obtained on the seminar.	

Metoda obliczania oceny końcowej	Sem.	Przedmiot	Rodzaj zaliczenia	Metoda obl. oceny	Waga do średniej
	6	cryptography (kryptografia)		Nieobliczana	
	6	cryptography (kryptografia) [konwersatorium]	zaliczenie z oceną		

Literatura podstawowa	J. A. Buchmann (2004): Introduction to Cryptography. Undergraduate Texts in Mathematics, Springer
Literatura uzupełniająca	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

NAKŁAD PRACY STUDENTA

	Liczba godzin	
		W tym e-learning
Zajęcia dydaktyczne	**30**	**0**
Udział w egzaminie/zaliczeniu	**4**	**0**
Przygotowanie się do zajęć	**20**	**0**
Studiowanie literatury	**20**	**0**
Udział w konsultacjach	**16**	**0**
Przygotowanie projektu / eseju / itp.	**0**	**0**
Przygotowanie się do egzaminu/zaliczenia	**10**	**0**
ŁĄCZNY nakład pracy studenta w godz.	**100**	
Liczba punktów ECTS	**4**	

COURSE SYLLABUS AND SPECIFICATION

Curriculum title: **USWN-M-O-II-S-19/20Z**						
Unit: **Moduł 3 [moduł]**						
Course title: **Entire and meromorphic functions (PODSTAWOWE)**					Course code: **WN17AIIJ2799_37S**	
Name of field of study: **matematyka**						
Mode and cycle of study: **second degree, full - time**		Profile of study: **general academic**		Specialty:		
Course / module status **elective**		Language of instruction: **semestr: 2 - english language (100%)**				
Year	**Semester**	**Form of instruction**	**No. of hours**	w tym e-learning	**Type of credit**	**ECTS**
1	2	konwersatorium	30	0	pg	6
		lecture	30	0	e	
Total			**60**			**6**
Course / module coordinator	dr EWA CIECHANOWICZ					
Course instructor						
Course / module objectives	**Broadening and reinforcing knowledge and skills concerning the analysis of functions of a single complex variable. Presentation of basic notions of the theory of growth and value distribution of entire and meromorphic functions of a single variable.**					
Prerequisites	**Knowledge of basics of complex analysis with respect to functions of a single variable.**					

LEARNING OUTCOMES

Category	No.	Code	Description	Ref. to programme benchmarks
knowledge	1	EP1	A student has extended knowledge in the field of complex analysis.	K_W01 K_W03 K_W05
	2	EP2	A student knows the main conjectures and theorems of complex analysis	K_W01 K_W03 K_W05
	3	EP3	A student has deeper knowledge with respect to entire and meromorphic functions.	K_W03
	4	EP4	A student is able to understand formulation of the issues in the theory of entire and meromorphic functions which are a matter of current research.	K_W04
	5	EP5	A student knows the interrelations between complex analysis and other areas of research.	K_W05
skills	1	EP6	A student is able to prove theorems and disprove false conjectures in the field of complex analysis	K_U01 K_U02
	2	EP7	A student is well-versed in the methods of complex analysis.	K_U02
	3	EP8	A student is able to conduct proofs applying methods from other areas of mathematics.	K_U02
social competences	1	EP9	A student knows limitations of his/her knowledge and understands the need for further education.	K_K01
	2	EP10	A student is able to formulate questions leading to deepening of knowledge .	K_K01
	3	EP11	A student is able to formulate opinions about selected issues of complex analysis.	K_K02

CONTENT	Semester	No. of hours	w tym e-learning
Subject title: **Entire and meromorphic functions**			
Format of instruction: **lecture**			
1. **Meromorphic functions. Poisson-Jensen formula.**	2	2	
2. **The first fundamental theorem of Nevanlinna.**	2	2	
3. **Charateristic of a meromorphic function. Properties of characteristic function. Characteristics of an entire function**	2	2	
4. **Order of a meromorphic function. Categories of growth.**	2	2	
5. **The theorem of Hadamard-Nevanlinna on representation of a meromorphic function of finite order according to its zeros and poles. Examples.**	2	4	
6. **Weierstrass product for a meromorphic function of a fixed order.**	2	4	
7. **The lemma on the logarithmic derivative**	2	2	
8. **The second fundamental theorem of Nevanlinna. Defect of a meromorphic function. The theorem on defects and Picard?s theorem.**	2	4	
9. **Deviation of a meromorphic function. Petrenko?s theory.**	2	4	
10. **Asymptotic values of entire and meromorphic fuctions. Denjoy-Carleman-Ahlfors theorem.**	2	2	
11. **Strong asymptotic values of meromorphic functions.**	2	2	
Format of instruction: **konwersatorium**			
1. **Meromorphic functions. Poisson-Jensen formula.**	2	2	
2. **The first fundamental theorem of Nevanlinna.**	2	2	
3. **Charateristic of a meromorphic function. Properties of characteristic function. Characteristics of an entire function**	2	2	
4. **Order of a meromorphic function. Categories of growth.**	2	2	
5. **The theorem of Hadamard-Nevanlinna on representation of a meromorphic function of finite order according to its zeros and poles. Examples.**	2	4	
6. **Weierstrass product for a meromorphic function of a fixed order.**	2	4	
7. **The lemma on the logarithmic derivative**	2	2	
8. **The second fundamental theorem of Nevanlinna. Defect of a meromorphic function. The theorem on defects and Picard?s theorem.**	2	4	
9. **Deviation of a meromorphic function. Petrenko?s theory.**	2	4	
10. **Asymptotic values of entire and meromorphic fuctions. Denjoy-Carleman-Ahlfors theorem.**	2	2	
11. **Strong asymptotic values of meromorphic functions.**	2	2	

Modes of delivery	**Lecture, explanation, discussion**	
Assessment methods		No. of learning outcome from the syllabus
	EGZAMIN PISEMNY	**EP1,EP2,EP3,EP4,EP5,EP6,EP7,EP8**
	SPRAWDZIAN	**EP1,EP2,EP3,EP4,EP5,EP6,EP7,EP8**
	ZAJĘCIA PRAKTYCZNE (WERYFIKACJA POPRZEZ OBSERWACJĘ)	**EP10,EP11,EP9**
Grading criteria	**To pass the workshop part of the course a student needs to pass the in-class tests.** **To pass the lecture part of the course a student needs to pass a written exam.** **To obtain the course credit a student needs to get positive grades from both parts.**	
	Grade calculation principles	
	The final grade for the course is an average of grades for both parts of the course.	

Final grade calculation method	Sem.	Course	Type of credit	Grade calc. method	Weight for the average
	2	Entire and meromorphic functions		Arytmetyczna	
	2	Entire and meromorphic functions [wykład]	egzamin		
	2	Entire and meromorphic functions [konwersatorium]	zaliczenie z oceną		

Basic reading	Conway, J. (1978): Functions of one complex variable, Springer
	Hayman, W.K. (1964): Meromorphic functions, Clarendon Press
	Leja, F. (1979): Funkcje zespolone, PWN
Supplementary reading	Petrenko, V.P. (1978): Growth of meromorphic functions, Vysha Shkola

STUDENT WORKLOAD

	No. of hours	
		W tym e-learning
Contact hours	**60**	
Participation in test / exam	**6**	
Preparation for contact hours	**30**	
Private reading and studying	**14**	
Participation in tutorials	**20**	
Preparation of project / essay / etc.	**0**	
Preparation for test / exam	**20**	
TOTAL workload	**150**	
ECTS credits	**6**	

COURSE SYLLABUS AND SPECIFICATION

Curriculum title: **USWN-M-O-II-S-19/20Z**						
Unit: **Moduł 2 [moduł]**						
Course title: **General measure theory (PODSTAWOWE)**					Course code: **WN17AIIJ2797_33S**	
Name of field of study: **matematyka**						
Mode and cycle of study: **second degree, full - time**		Profile of study: **general academic**		Specialty:		
Course / module status **elective**		Language of instruction: **semestr: 1 - english language (100%)**				
Year	**Semester**	**Form of instruction**	**No. of hours**	**w tym e-learning**	**Type of credit**	**ECTS**
1	1	konwersatorium	30	0	pg	6
		lecture	30	0	e	
Total			**60**			**6**
Course / module coordinator	**dr hab. FRANCISZEK PRUS-WIŚNIOWSKI**					
Course instructor						
Course / module objectives	**The main purpose is to acquaint students with general measure theory and general integral theory. The workshops aim at gaining good grasp of basic concepts and methods of proving as well as providing more detailed information on some topics.**					
Prerequisites	**The Lebesgue measure and integral on real line. Elements of topology and of metric spaces.**					

LEARNING OUTCOMES

Category	**No.**	**Code**	**Description**	Ref. to programme benchmarks
knowledge	1	EP1	manifests an in-depth knowledge of the basic branches of mathematics	K_W01
	2	EP2	understands well the role and importance of the construction of mathematical reasoning	K_W02
	3	EP3	knows the most important theorems and hypotheses of main branches of mathematics	K_W01
	4	EP4	has an in-depth knowledge of the selected field of mathematics: knows most classical definitions and theorems and their proofs	K_W03
	5	EP5	knows connections of the issues of a selected field with other fields of theoretical and applied mathematics	K_W03 K_W04

skills	1	EP6	is able to construct mathematical reasoning: proving theorems and refuting hypotheses by construction and selection of counter-examples	K_U01 K_U02 K_U13
	2	EP7	has the ability to express mathematical contents in speech and writing, in mathematical texts of different nature	K_U11 K_U13
	3	EP8	has the ability to validate inferences in constructing formal proofs	K_U01 K_U13
	4	EP9	knows the construction of Lebesgue?s measure and integral; can use the concept of the measure theory in typical theoretical and practical issues	K_U04 K_U13
	5	EP10	has the ability to recognise topological structures in mathematical objects. e.g. in geometry or mathematical analysis; can use the basic topological properties of sets, functions and transformations	K_U05 K_U13
	6	EP11	can examine in the selected field the proofs in which, if necessary, uses also the tools of other branches of mathematics	K_U01 K_U13
	7	EP14	can work in a team; understands the necessity of working systematically on all projects which are long-term in nature	K_U13 K_U15
social competences	1	EP12	is aware of the limitations of his / her own knowledge and understands the need of further education	K_K01 K_K04
	2	EP13	is ready to precisely formulate the questions which are aimed at increasing his / her own understanding of a given topic or finding the missing elements of reasoning	K_K01 K_K02

CONTENT	Semester	No. of hours	w tym e-learning
Subject title: **General measure theory**			
Format of instruction: **lecture**			
1. **General measure spaces (measures, signed measures, Hahn and Jordan decompositions, construction of outer measures, theorems of extension to measures)**	1	12	
2. **Integration with respect to general measures (meaurable functions, integral of nonnegative function, integral of arbitrary function, Lebesgue-Stieltjes integral, the Vitali-Hahn-Saks theorem)**	1	12	
3. **Some more important measures (the Lebesgue measure in euclidean spaces, change of variable in the Lebesgue integral, the Lebesgue-Stieltjes integral, Borel measures)**	1	6	
Format of instruction: **konwersatorium**			
1. **General measure spaces**	1	12	
2. **Integration with respect to general measures**	1	12	
3. **Some more important measures**	1	6	

Modes of delivery	**Lecture, explanations, discussion, written description of some solutions**	
Assessment methods		No. of learning outcome from the syllabus
	EGZAMIN USTNY	**EP1,EP10,EP11,EP2,EP3,EP4,EP5,EP6,EP7,EP8,EP9**
	SPRAWDZIAN	**EP1,EP10,EP3,EP4,EP6,EP7,EP8,EP9**
	ZAJĘCIA PRAKTYCZNE (WERYFIKACJA POPRZEZ OBSERWACJĘ)	**EP1,EP10,EP11,EP12,EP13,EP14,EP2,EP3,EP4,EP5,EP6,EP7,EP8,EP9**

Grading criteria	**The workshops are graded based on written in-class test with open problems and on observation of activity throughout the semester and on grades from selected written home assignements.** **The lecture is graded based on oral exam.**
	Grade calculation principles
	The final grade is the weighted arithmetic average from grades from all formats of instruction.

Final grade calculation method	Sem.	Course	Type of credit	Grade calc. method	Weight for the average
	1	General measure theory		Arytmetyczna	
	1	General measure theory [konwersatorium]	zaliczenie z oceną		
	1	General measure theory [wykład]	egzamin		

Basic reading	Royden H.L., Fitzpatrick P. (1998): Real Analysis, Macmillan Publishing Company
Supplementary reading	Yeh J. (2008): Real Analysis, World Scientific

STUDENT WORKLOAD

	No. of hours	
		W tym e-learning
Contact hours	**60**	
Participation in test / exam	**10**	
Preparation for contact hours	**30**	
Private reading and studying	**20**	
Participation in tutorials	**10**	
Preparation of project / essay / etc.	**0**	
Preparation for test / exam	**20**	
TOTAL workload	**150**	
ECTS credits	**6**	