

KARTA PRZEDMIOTU

Kod przedmiotu	11.1-2MAT-F02.2-K	
Nazwa przedmiotu w języku	polskim	Kryptografia
	angielskim	Cryptography

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	<i>matematyka</i>
1.2. Forma studiów	<i>studia stacjonarne / studia niestacjonarne</i>
1.3. Poziom studiów	<i>studia drugiego stopnia</i>
1.4. Profil studiów	<i>ogólnoakademicki</i>
1.5. Specjalność	<i>nauczanie matematyki, zastosowania matematyki</i>
1.6. Jednostka prowadząca przedmiot	<i>WM, Instytut Matematyki</i>
1.7. Osoba przygotowująca kartę przedmiotu	<i>prof. dr hab. Taras Banakh, dr Joanna Garbulińska-Węgrzyn, dr hab. Andrzej Chrzęszczuk</i>
1.8. Osoba odpowiedzialna za przedmiot	<i>dr hab. Cornelia Schiebold</i>
1.9. Kontakt	

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Przynależność do modułu	<i>F</i>
2.2. Status przedmiotu	<i>Fakultatywny</i>
2.3. Język wykładowy	<i>Polski</i>
2.4. Semestry, na których realizowany jest przedmiot	<i>4</i>
2.5. Wymagania wstępne	<i>Algebra z teorią liczb</i>

3. FORMY, SPOSOBY I METODY PROWADZENIA ZAJĘĆ

3.1. Formy zajęć	<i>wykład (30 – studia stacjonarne, 10 – studia niestacjonarne), ćwiczenia laboratoryjne (30 – studia stacjonarne, 15 – studia niestacjonarne)</i>	
3.2. Sposób realizacji zajęć	<i>zajęcia w pomieszczeniu dydaktycznym UJK</i>	
3.3. Sposób zaliczenia zajęć	<i>zaliczenie z oceną (wykład), zaliczenie z oceną (ćwiczenia laboratoryjne)</i>	
3.4. Metody dydaktyczne	<i>wykład - wykład, dyskusja, praca z książką ćwiczenia laboratoryjne – dyskusja, rozwiązywanie zadań, praca na komputerze, projekt, praca z książką</i>	
3.5. Wykaz literatury	podstawowa	<i>Chrzęszczuk A. Algorytmy teorii liczb i kryptografii. BTC. Legionowo 2010 Koblitz N. Wykład z teorii liczb i kryptografii. WNT. Warszawa 1995 Blake I., Seroussi G., Smart N. Krzywe eliptyczne w kryptografii. WNT. Warszawa 2005</i>
	uzupełniająca	<i>Koblitz N, Algebraiczne aspekty kryptografii. WNT. Warszawa 2000 Menezes A. J. i in. Kryptografia stosowana. WNT. Warszawa 2005 Stinson D. R. Kryptografia w teorii i praktyce. WNT. Warszawa 2005 Schneier B. Kryptografia dla praktyków. WNT. Warszawa 2002</i>

4. CELE, TREŚCI I EFEKTY KSZTAŁCENIA

4.1. Cele przedmiotu
Wiedza: C1 - Zapoznanie z zastosowaniami algebry i geometrii algebraicznej w kryptografii.
Umiejętności: C2 - Umiejętność praktycznego wykorzystania zdobytej wiedzy oraz zastosowanie pakietów obliczeniowych.
Kompetencje społeczne: C3 - Rozumie potrzebę ciągłego uczenia się.

4.2. Treści programowe

Wykład: Rozwinięcia liczb przy danej podstawie. Kodowanie tekstu przy pomocy liczb. Efektywna arytmetyka w ciałach skończonych: dodawanie, mnożenie, inwersja i potęgowanie. Faktoryzacja i problem logarytmu dyskretnego. Kryptosystemy RSA i ElGamala w ciałach skończonych. Podpisy cyfrowe.

Podstawowe własności krzywych eliptycznych nad ciałami skończonymi: działanie grupowe. Zastosowanie krzywych eliptycznych do szyfrowania z kluczem publicznym i podpisów cyfrowych. Przewaga nad RSA i w ciałami skończonymi. Wykorzystanie pakietów obliczeniowych.

Ćwiczenia laboratoryjne: Rozwinięcia liczb przy danej podstawie. Kodowanie tekstu przy pomocy liczb. Efektywna arytmetyka w ciałach skończonych: dodawanie, mnożenie, inwersja i potęgowanie. Faktoryzacja i problem logarytmu dyskretnego. Kryptosystemy RSA i ElGamala w ciałach skończonych. Podpisy cyfrowe. Podstawowe własności krzywych eliptycznych nad ciałami skończonymi: działania grupowe. Zastosowanie krzywych eliptycznych do szyfrowania z kluczem publicznym i podpisów cyfrowych. Przewaga nad RSA i w ciałami skończonymi. Wykorzystanie pakietów obliczeniowych.

4.3. Przedmiotowe efekty kształcenia (mała, średnia, duża liczba efektów)

kod	Student, który zaliczył przedmiot	Stopień nasycenia efektu kierunkowego	Odniesienie do efektów kształcenia	
	w zakresie WIEDZY:		dla kierunku	dla obszaru
W01	stosuje teorię ciał skończonych i krzywych eliptycznych w kryptografii,	++ ++	MAT2A_W02 MAT2A_W03	X2A_W02 X2A_W06
W02	posługuje się wybranymi algorytmami algebry i ich zastosowaniami w kryptografii,	++	MAT2A_W06	X2A_W03 X2A_W04
W03	stosuje poznaną wiedzę wykorzystując pakiety do obliczeń symbolicznych.	++	MAT2A_W07	X2A_W04 X2A_W05
	w zakresie UMIEJĘTNOŚCI:			
U01	w praktyce stosuje poznaną wiedzę z algebry i geometrii do zaszyfrowania wiadomości i podpisów cyfrowych,	++	MAT2A_U02	X2A_U03 X2A_U05
U02	dostrzega struktury algebraiczne i geometryczne w kryptografii. potrafi stosować wybrane pojęcia algebry, teorii liczb i geometrii w praktyce,	++ ++	MAT2A_U04 MAT2A_U13	X2A_U03 X2A_U01 X2A_U02 X2A_U05
U03	konstruuje grupy ilorazowe, ciała skończone i krzywe eliptyczne wykorzystywane do szyfrowania,	++	MAT2A_U15	X2A_U02 X2A_U04 X2A_U06
U04	rozpoznaje problemy, w tym zagadnienia praktyczne, które można rozwiązać algorytmicznie.	++	MAT2A_U19	X2A_U04
	w zakresie KOMPETENCJI SPOŁECZNYCH:			
K01	planuje swoją pracę,	++	MAT2A_K01	X2A_K03
K02	pracuje w grupie, współpracuje z jej członkami w celu opracowania złożonych algorytmów.	++	MAT2A_K03	X2A_K02

4.4. Kryteria oceny osiągniętych efektów kształcenia dla każdej formy zajęć

na ocenę 3	na ocenę 3,5	na ocenę 4	na ocenę 4,5	na ocenę 5
Zaliczenie ćwiczeń laboratoryjnych: osiąga 50-60% liczby punktów możliwych do uzyskania z kolokwium, projektu i	Zaliczenie ćwiczeń laboratoryjnych: osiąga 61-70% liczby punktów możliwych do uzyskania z kolokwium, projektu	Zaliczenie ćwiczeń laboratoryjnych: osiąga 71-80% liczby punktów możliwych do uzyskania z kolokwium, projektu	Zaliczenie ćwiczeń laboratoryjnych: osiąga 81-90% liczby punktów możliwych do uzyskania z kolokwium, projektu	Zaliczenie ćwiczeń laboratoryjnych: osiąga 91-100% liczby punktów możliwych do uzyskania z kolokwium, projektu

aktywności na zajęciach. Zaliczenie wykładu: osiąga 50-60 % punktów z kolokwium.	i aktywności na zajęciach. Zaliczenie wykładu: osiąga 61-70 % punktów z kolokwium..	i aktywności na zajęciach. Zaliczenie wykładu: osiąga 71-80 % punktów z kolokwium..	i aktywności na zajęciach. Zaliczenie wykładu: osiąga 81-90 % punktów z kolokwium.	i aktywności na zajęciach. Zaliczenie wykładu: osiąga 91-100 % punktów z kolokwium.
--	---	---	--	---

4.5. Metody oceny dla każdej formy zajęć							
Egzamin ustny	Egzamin pisemny	Projekt	Kolokwium	Zadania domowe	Referat Sprawozdania	Dyskusje	Inne ¹
		x(ćw.lab.)	x(wyk., ćw.lab)	x(ćw.lab)		x(w, ćw.lab)	

5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta	
	Studia Stacjonarne	Studia niestacjonarne
LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/	60	25
Udział w wykładach	30	10
Udział w ćwiczeniach, konwersatoriach, laboratoriach... itd.	30	15
Udział w konsultacjach		
Udział w egzaminie/kolokwium zaliczeniowym itp.		
Inne		
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	65	100
Przygotowanie do wykładu	10	30
Przygotowanie do ćwiczeń, konwersatorium, laboratorium itp.	15	25
Przygotowanie do egzaminu/kolokwium	25	25
Zebranie materiałów do projektu, kwerenda internetowa	15	20
Opracowanie prezentacji multimedialnej		
Przygotowanie hasła do wikipedii		
Inne		
ŁĄCZNA LICZBA GODZIN	125	125
PUNKTY ECTS za przedmiot	5	5

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot w danym roku akademickim)

.....