KARTA PRZEDMIOTU

Kod przedmiotu	0541-2MAT-F56-K	
Nazwa przedmiotu w języku	polskim	***Kryptografia***
	angielskim	***Cryptography***

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	matematyka
1.2. Forma studiów	studia stacjonarne
1.3. Poziom studiów	studia drugiego stopnia
1.4. Profil studiów	ogólnoakademicki
1.5. Specjalność	nauczanie matematyki, analiza danych
1.6. Jednostka prowadząca przedmiot	WM, Instytut Matematyki
1.7. Osoba/zespół przygotowująca/y kartę przedmiotu	prof. zw dr hab. Taras Banakh, prof. UJK dr hab. Andrzej Chrzęszczyk, dr Joanna Garbulińska-Węgrzyn
1.8. Osoba odpowiedzialna za przedmiot	
1.9. Kontakt	

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Przynależność do modułu	Fakultatywny
2.2. Język wykładowy	polski
2.3. Semestry, na których realizowany jest przedmiot	4
2.4. Wymagania wstępne	Algebra z teorią liczb

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Forma zajęć		wykład, ćwiczenia laboratoryjne
3.2. Miejsce realizacji zajęć		zajęcia w po mieszczeniu dydaktycznym UJK
3.3. Forma zaliczenia zajęć		zaliczenie z oceną (wykład, ćwiczenia laboratoryjne)
3.4. Metody dydaktyczne		wykład – wykład, dyskusja, praca z książką ćwiczenia laboratoryjne – dyskusja, rozwiązywanie zadań, praca na komputerze, projekt, praca z książką
3.5. Wykaz literatury	**podstawowa**	Chrzęszczyk 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
	uzupełniająca	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

4. CELE, TREŚCI I EFEKTY KSZTAŁCENIA

4.1. Cele przedmiotu *(z uwzględnieniem formy zajęć)*

Wykład

C1 – zapoznanie z zastosowaniami algebry i geometrii algebraicznej w kryptografii

Ćwiczenia laboratoryjne

C1 – kształcenie umiejętności praktycznego wykorzystania zdobytej wiedzy oraz zastosowanie pakietów obliczeniowych

C2 –uświadomienie potrzeby ciągłego uczenia się

4.2. Treści programowe *(z uwzględnieniem formy zajęć)*

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 szyfrowanie 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 szyfrowanie z kluczem publicznym i podpisów cyfrowych. Przewaga nad RSA i w ciałami skończonymi. Wykorzystanie pakietów obliczeniowych.

4.3. Przedmiotowe efekty kształcenia

Efekt	Student, który zaliczył przedmiot	Odniesienie do kierunkowych efektów kształcenia
w zakresie **WIEDZY:**		
W01	stosuje teorię ciał skończonych i krzywych eliptycznych w kryptografii	MAT2A_W02 MAT2A_W03
W02	posługuje się wybranymi algorytmami algebry i ich zastosowaniami w kryptografii	MAT2A_W05
W03	stosuje poznaną wiedzę wykorzystując pakiety do obliczeń symbolicznych	MAT2A_W06
w zakresie **UMIEJĘTNOŚCI:**		
U01	w praktyce stosuje poznaną wiedzę z algebry i geometrii do zaszyfrowania wiadomości i podpisów cyfrowych	MAT2A_U02
U02	dostrzega struktury algebraiczne i geometryczne w kryptografii. potrafi stosować wybrane pojęcia algebry, teorii liczb i geometrii w praktyce	MAT2A_U03 MAT2A_U12
U03	konstruuje grupy ilorazowe, ciała skończone i krzywe eliptyczne wykorzystywane do szyfrowania	MAT2A_U14
U04	rozpoznaje problemy, w tym zagadnienia praktyczne, które można rozwiązać algorytmicznie	MAT2A_U18
U05	pracuje w grupie, współpracuje z jej członkami w celu opracowania złożonych algorytmów	MAT2A_U24
w zakresie **KOMPETENCJI SPOŁECZNYCH:**		
K01	planuje swoją pracę	MAT2A_K01

4.4. Sposoby weryfikacji osiągnięcia przedmiotowych efektów kształcenia

Efekty przedmiotowe *(symbol)*	Sposób weryfikacji (+/-)					
	Kolokwium		Projekt		Zadania domowe	
	Forma zajęć		*Forma zajęć*		*Forma zajęć*	
	W	*C*	*W*	*C*	*W*	*C*
W01	+					
W02	+					
W03	+					
U01		+		+		+
U02		+		+		+
U03		+		+		+
U04		+		+		+
U05				+		+
K01				+		+

4.5. Kryteria oceny stopnia osiągnięcia efektów kształcenia

Forma zajęć	Ocena	Kryterium oceny
wykład (*W*)	**3**	co najmniej 50% i nie więcej, niż 60% łącznej liczby punktów możliwych do uzyskania
	3,5	ponad 60% i nie więcej, niż 70% łącznej liczby punktów możliwych do uzyskania
	4	ponad 70% i nie więcej, niż 80% łącznej liczby punktów możliwych do uzyskania
	4,5	ponad 80% i nie więcej, niż 90% łącznej liczby punktów możliwych do uzyskania
	5	ponad 90% liczby punktów możliwych do uzyskania
ćwiczenia laboratoryjne (*C*)	**3**	co najmniej 50% i nie więcej, niż 60% łącznej liczby punktów możliwych do uzyskania
	3,5	ponad 60% i nie więcej, niż 70% łącznej liczby punktów możliwych do uzyskania
	4	ponad 70% i nie więcej, niż 80% łącznej liczby punktów możliwych do uzyskania
	4,5	ponad 80% i nie więcej, niż 90% łącznej liczby punktów możliwych do uzyskania
	5	ponad 90% liczby punktów możliwych do uzyskania

5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
	Studia stacjonarne
LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/	***60***
Udział w wykładach	30
Udział w ćwiczeniach laboratoryjnych	30
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	***40***
Przygotowanie do ćwiczeń laboratoryjnych	15
Przygotowanie do kolokwium	15
Przygotowanie projektu	10
ŁĄCZNA LICZBA GODZIN	***100***
PUNKTY ECTS za przedmiot	**4**

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

.....