KARTA PRZEDMIOTU

Kod przedmiotu	**11.1-2MAT-F02.1-PK**	
Nazwa przedmiotu w języku	polskim	**Podstawy kryptografii**
	angielskim	**The basics of cryptography**

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	*matematyka*
1.2. Forma studiów	*studia stacjonarne / studia niestacjonarne*
1.3. Poziom studiów	*studia pierwszego stopnia licencjackie*
1.4. Profil studiów	*ogólnoakademicki*
1.5. Specjalność	*nauczanie matematyki, zastosowania matematyki*
1.6. Jednostka prowadząca przedmiot	*WM, Instytut Matematyki*
1.7. Osoba przygotowująca kartę przedmiotu	*prof. dr hab. Taras Banakh, dr Joanna Garbulińska-Węgrzyn dr hab. Andrzej Chrzęszczyk*
1.8. Osoba odpowiedzialna za przedmiot	*dr hab. Andrzej Chrzęszczyk*
1.9. Kontakt	*achrzesz@ujk.edu.pl*

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Przynależność do modułu	*F*
2.2. Status przedmiotu	*fakultatywny*
2.3. Język wykładowy	*polski*
2.4. Semestry, na których realizowany jest przedmiot	*6*
2.5. Wymagania wstępne	*Algebra z teorią liczb*

3. FORMY, SPOSOBY I METODY PROWADZENIA ZAJĘĆ

3.1. Formy zajęć		*wykład (30 – studia stacjonarne, 10 – studia niestacjonarne), ćwiczenia laboratoryjne (30 – studia stacjonarne, 15 – studia niestacjonarne)*
3.2. Sposób realizacji zajęć		*zajęcia w pomieszczeniu dydaktycznym UJK*
3.3. Sposób zaliczenia zajęć		*zaliczenie z oceną (wykład), zaliczenie z oceną (ćwiczenia laboratoryjne)*
3.4. Metody dydaktyczne		*wykład - wykład, dyskusja, praca z książką ćwiczenia laboratoryjne – dyskusja, rozwiązywanie zadań, 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*
	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*

4. CELE, TREŚCI I EFEKTY KSZTAŁCENIA

4.1. Cele przedmiotu

Wiedza:

C1 **-** Zapoznanie z podstawowymi metodami stosowanymi w kryptografii.

Umiejętności:

C2 **-** Rozwijanie umiejętności implementacji algorytmów i zastosowania zdobytej wiedzy z wykorzystaniem 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. Szyfry symetryczne, wkład matematyków polskich w złamanie Enigmy. Kryptosystem RSA. Konstruowanie ciał skończonych. Efektywna arytmetyka w ciałach skończonych.. Problem logarytmu dyskretnego w ciałach skończonych. Schemat wymiany kluczy Diffiego-Hellmana, Kryptosystem ElGamala, podpisy cyfrowe. Zastosowania krzywych eliptycznych w kryptografii.

Ćwiczenia laboratoryjne: Rozwinięcia liczb przy danej podstawie, kodowanie tekstu przy pomocy liczb. Przykłady szyfrowania symetrycznego. Szyfrowanie RSA.

Konstruowanie ciał skończonych. Efektywna arytmetyka w ciałach skończonych. Kryptosystem ElGamala, podpisy cyfrowe. Rozwiązywania problemu logarytmu dyskretnego.Wykorzystanie krzywych eliptycznych. Zapisywanie algorytmów w pseudokodzie i implementacja wybranym języku programowania. 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	rozumie cywilizacyjne znaczenie matematyki i jej zastosowań w kryptografii,	++	MAT1A_W01	X1A_W01
W02	definiuje podstawy technik obliczeniowych programowania, wspomagających pracę matematyka i rozumie ich ograniczenia,	++ ++	MAT1A_W08 MAT1A_W16	X1A_W04 X1A_W05
W03	posługuje się na poziomie podstawowym co najmniej jednym pakietem oprogramowania służącym do obliczeń symbolicznych (Magma lub Sage)	++	MAT1A_W09	X1A_W05
	w zakresie **UMIEJĘTNOŚCI:**			
U01	tworzy ciała skończone drogą konstruowania pierścieni ilorazowych,	++	MAT1A_U04	X1A_U01
U02	dostrzega obecność i rolę struktur algebraicznych w kryptografii (np. ciał skończonych),	++	MAT1A_U14	X1A_U01 X1A_U07
U03	rozpoznaje problemy związane z szyfrowaniem, które można rozwiązać algorytmicznie	++	MAT1A_U21	X1A_U04
	w zakresie **KOMPETENCJI SPOŁECZNYCH:**			
K01	planuje swoją pracę	++	MAT1A_K01	X1A_K03
K02	pracuje w grupie, współpracuje z jej członkami w celu opracowania złożonych algorytmów.	++	MAT1A_K03	X1A_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 **Zaliczenie wykładu:** osiąga 50%-60% liczby punktów z kolokwium	**Zaliczenie ćwiczeń laboratoryjnych:** osiąga 61%-70% liczby punktów możliwych do uzyskania **Zaliczenie wykładu:** osiąga 61%-70% liczby punktów z kolokwium	**Zaliczenie ćwiczeń laboratoryjnych:** osiąga 71%-80% liczby punktów możliwych do uzyskania **Zaliczenie wykładu:** osiąga 71%-80% liczby punktów z kolokwium	**Zaliczenie ćwiczeń laboratoryjnych:** osiąga 81%-90% liczby punktów możliwych do uzyskania **Zaliczenie wykładu:** osiąga 81%-90% liczby punktów z kolokwium	**Zaliczenie ćwiczeń laboratoryjnych:** osiąga 91%-100% liczby punktów możliwych do uzyskania **Zaliczenie wykładu:** osiąga 91%-100% liczby 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. w)*	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	25
Przygotowanie do ćwiczeń, konwersatorium, laboratorium itp.	10	30
Przygotowanie do egzaminu/kolokwium	25	25
Zebranie materiałów do projektu, kwerenda internetowa	20	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)*

.....