KARTA PRZEDMIOTU

Kod przedmiotu	0541.6.MAT2.C.ZMI	
Nazwa przedmiotu w języku	polskim	***Zastosowania matematyki w informatyce***
	angielskim	***Applications of mathematics in computer science***

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	matematyka
1.2. Forma studiów	studia stacjonarne
1.3. Poziom studiów	studia drugiego stopnia, magisterskie
1.4. Profil studiów*	ogólnoakademicki
1.5. Osoba przygotowująca kartę przedmiotu	dr Magdalena Nowak
1.6. Kontakt	mnowak@ujk.edu.pl

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Język wykładowy	polski
2.2. Wymagania wstępne*	Wstęp do matematyki, Algebra z teorią liczb

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Forma zajęć		wykład, konwersatorium
3.2. Miejsce realizacji zajęć		zajęcia w pomieszczeniu dydaktycznym UJK
3.3. Forma zaliczenia zajęć		zaliczenie z oceną
3.4. Metody dydaktyczne		wykład-wykład konwersatoryjny, ćwiczenia laboratoryjne- dyskusja rozwiązywanie zadań, praca na komputerze
3.5. Wykaz literatury	**podstawowa**	Knuth D. E., Sztuka programowania. tom 2. WNT. 2000 Yan S. Y., Teoria liczb w informatyce. PWN. Warszawa 2006 Graham R. L., Knuth D. E., Patashnik O., Matematyka konkretna. PWN. 2011
	uzupełniająca	Kisielewicz A., Sztuczna inteligencja i logika. WNT. Warszawa 2011 von zur Gathen J., Gerhard J., Modern Computer Algebra. Cambridge University Press. Second edition. 2003

4. CELE, TREŚCI I EFEKTY UCZENIA SIĘ

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

Wykład:

C1 – Rozszerzenie wiadomości z podstawowego kursu algebry z teorią liczb oraz wstępu do matematyki.

Konwersatorium:

C2 - Rozwijanie umiejętności samodzielnej implementacji algorytmów i zastosowania zdobytej wiedzy z wykorzystaniem pakietów obliczeniowych.

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

Wykład:

1. Elementy teorii informacji: entropia, redundancja.
2. Układy logiczne i funkcje boolowskie.
3. Kodowanie informacji. Rozwinięcia liczb przy danej podstawie. Kodowanie tekstu przy pomocy liczb.
4. Elementy kryptografii.
5. Efektywna arytmetyka w ciałach skończonych: dodawanie, mnożenie, inwersja i potęgowanie.
6. Faktoryzacja i problem logarytmu dyskretnego.
7. Kryptosystemy RSA i ElGamala w ciałach skończonych. Podpisy cyfrowe.
8. Podstawowe własności krzywych eliptycznych nad ciałami skończonymi: działanie grupowe.

Ćwiczenia laboratoryjne:

1. Układy logiczne i funkcje boolowskie.
2. Kodowanie informacji. Rozwinięcia liczb przy danej podstawie. Kodowanie tekstu przy pomocy liczb.
3. Analiza kryptosystemów RSA i ElGamala w ciałach skończonych. Podpisy cyfrowe.
4. Zastosowanie krzywych eliptycznych do szyfrowania z kluczem publicznym i podpisów cyfrowych. Wykorzystanie pakietów obliczeniowych.

4.3. Przedmiotowe efekty uczenia się

Efekt	**Student, który zaliczył przedmiot**	**Odniesienie do kierunkowych efektów uczenia się**
w zakresie **WIEDZY:**		

W01	wymienia wybrane algorytmy algebry i zna ich zastosowania,	MAT2A_W04 MAT2A_W07
W02	stosuje teorię ciał skończonych i krzywych eliptycznych w kryptografii,	MAT2A_W04 MAT2A_W07
W03	posługuje się na poziomie podstawowym co najmniej jednym pakietem oprogramowania służącym do obliczeń symbolicznych	MAT2A_W04 MAT2A_W05
w zakresie **UMIEJĘTNOŚCI:**		
U01	w praktyce stosuje poznaną wiedzę z algebry i geometrii do zaszyfrowania wiadomości i podpisów cyfrowych,	MAT2A_U11
U02	konstruuje grupy ilorazowe, ciała skończone i krzywe eliptyczne wykorzystywane do szyfrowania	MAT2A_U11
U03	rozpoznaje problemy, w tym zagadnienia praktyczne, które można rozwiązać algorytmicznie.	MAT2A_U11
U04	zapisuje algorytmy w wybranym języku programowania, kompiluje, uruchomia i testuje napisany samodzielnie program komputerowy	MAT2A_U15
w zakresie **KOMPETENCJI SPOŁECZNYCH:**		
K01	planuje swoją pracę	MAT2A_K01

4.4. Sposoby weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe *(symbol)*	**Sposób weryfikacji (+/-)**																							
	Egzamin ustny/pisemny*			**Kolokwium***			**Projekt***			**Aktywność na zajęciach***			**Praca własna***			**Praca w grupie***			**Inne *(jakie?)****				
	Forma zajęć			***Forma zajęć***			***Forma zajęć***			***Forma zajęć***			***Forma zajęć***			***Forma zajęć***			***Forma zajęć***				
	W	*C*	*...*	*W*	*C*	*...*	*W*	*C*	*...*	*W*	*C*	*...*	*W*	*C*	*...*	*W*	*C*	*...*	*W*	*C*	*...*		
W01				+				+		+	+		+	+										
W02				+				+		+	+		+	+										
W03				+				+		+	+		+	+										
U01					+			+		+	+		+	+										
U02					+			+		+	+		+	+										
U03					+			+		+	+		+	+										
U04					+			+		+	+		+	+										
K01					+			+		+	+		+	+										

niepotrzebne usunąć

4.5. Kryteria oceny stopnia osiągnięcia efektów uczenia się

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% łącznej 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% łącznej liczby punktów możliwych do uzyskania

5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	**Obciążenie studenta**	
	Studia stacjonarne	**Studia niestacjonarne**
LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/	***47***	
*Udział w wykładach**	15	
*Udział w ćwiczeniach, konwersatoriach, laboratoriach**	30	
*Udział w egzaminie/kolokwium zaliczeniowym**	2	
*Inne (jakie?)**		
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	***28***	
*Przygotowanie do wykładu**		

*Przygotowanie do ćwiczeń, konwersatorium, laboratorium**	20	
*Przygotowanie do egzaminu/kolokwium**	8	
*Zebranie materiałów do projektu, kwerenda internetowa**		
*Opracowanie prezentacji multimedialnej**		
*Inne (należy wskazać jakie? np. e-learning)**		
ŁĄCZNA LICZBA GODZIN	***75***	
PUNKTY ECTS za przedmiot	**3**	

niepotrzebne usunąć

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

.....