KARTA PRZEDMIOTU

Kod przedmiotu	0541.6.MAT1.D.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	stacjonarne
1.3. Poziom studiów	Studia pierwszego stopnia, licencjackie
1.4. Profil studiów*	ogólnoakademicki
1.5. Osoba przygotowująca kartę przedmiotu	Olena Karlova
1.6. Kontakt	olena.karlova@ujk.edu.pl

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Język wykładowy	polski
2.2. Wymagania wstępne*	Algebra abstrakcyjna 1 i 2

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Forma zajęć		wykład, konwersatorium
3.2. Miejsce realizacji zajęć		pomieszczenia dydaktyczne UJK
3.3. Forma zaliczenia zajęć		wykład: zal. z oceną, konwersatorium: zal. z oceną
3.4. Metody dydaktyczne		wykład akademicki, dyskusja, zajęcia warsztatowe (rozwiązywanie zadań)
3.5. Wykaz literatury	**podstawowa**	Chrzęszczyk A., Algorytmy teorii liczb i kryptografii. BTC. Legionowo 2010 Koblitz N., Algebraiczne aspekty kryptografii. WNT. Warszawa 2000
	uzupełniająca	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 UCZENIA SIĘ

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

Wykład:

C1 – zapoznanie z podstawowymi metodami stosowanymi w kryptografii

Ćwiczenia laboratoryjne:

C1 – rozwijanie umiejętności implementacji algorytmów i zastosowania zdobytej wiedzy z wykorzystaniem pakietów obliczeniowych

C2 – kształtowanie rozumienia potrzeby ciągłego uczenia się

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

Wykład:

Kryptografia z kluczem symetrycznym. System S-DES. Kryptografia z kluczem publicznym. Wymiana kluczy Diffiego-Hellmana. Systemy RSA, ElGamal. System plecakowy. Podpis cyfrowy RSA. Krzywe eliptyczne. Wymiana kluczy z wykorzystaniem krzywych eliptycznych. Podpis cyfrowy z wykorzystaniem krzywych eliptycznych. Metody faktoryzacji liczb całkowitych. Generacja liczb pseudolosowych.

Ćwiczenia laboratoryjne:

Kryptografia z kluczem symetrycznym. System S-DES. Kryptografia z kluczem publicznym. Wymiana kluczy Diffiego-Hellmana. Systemy RSA, ElGamal. System plecakowy. Podpis cyfrowy RSA. Krzywe eliptyczne. Wymiana kluczy z wykorzystaniem krzywych eliptycznych. Podpis cyfrowy z wykorzystaniem krzywych eliptycznych. Metody faktoryzacji liczb całkowitych. Generacja liczb pseudolosowych.

4.3. Przedmiotowe efekty uczenia się

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

W01	cywilizacyjne znaczenie matematyki i jej zastosowań w kryptografii	MAT1A_W01
W02	takie pojęcia kryptografii jak szyfrowanie z kluczem symetrycznym, szyfrowanie z kluczem publicznym, podpis cyfrowy	MAT1A_W04
w zakresie **UMIEJĘTNOŚCI** potrafi:		
U01	wykorzystać metody szyfrowania z kluczem symetrycznym i publicznym do ochrony danych oraz metody podpisu cyfrowego do potwierdzenia tożsamości	MAT1A_U13 MAT1A_W19
U02	realizować algorytmy szyfrowania i podpisu cyfrowego za pomocą wybranego języka programowania	MAT1A_W16 MAT1A_U11
U03	rozpoznać problemy związane z szyfrowaniem, które można rozwiązać algorytmicznie	MAT1A_U11 MAT1A_U13
w zakresie **KOMPETENCJI SPOŁECZNYCH** jest gotów do:		
K01	precyzyjnego formułowania pytań służących pogłębieniu własnego zrozumienia danego tematy lub odnalezieniu brakujących elementów rozumowania	MAT1A_K02

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				+	+					+	+										
U01					+					+	+										
U02					+					+	+										
U03					+					+	+										
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
konwersatorium (*K*)	**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/	***77***	
*Udział w wykładach**	30	
*Udział w ~~ćwiczeniach~~, konwersatoriach, ~~laboratoriach~~**	45	

*Udział w ~~egzaminie~~/kolokwium zaliczeniowym**	2	
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	***48***	
*Przygotowanie do wykładu**	15	
*Przygotowanie do ~~ćwiczeń~~, konwersatorium,~~ laboratorium~~**	20	
*Przygotowanie do ~~egzaminu~~/kolokwium zaliczeniowego**	13	
ŁĄCZNA LICZBA GODZIN	***125***	
PUNKTY ECTS za przedmiot	**5**	

niepotrzebne usunąć

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

……