Zał. nr 5 do ZW 13/2019
Załącznik nr ..... do programu studiów

WYDZIAŁ PODSTAWOWYCH PROBLEMÓW TECHNIKI

KARTA PRZEDMIOTU

Nazwa w języku polskim	:	**Algebraiczne aspekty kryptografii**
Nazwa w języku angielskim	:	**Algebraic aspects of cryptography**
Kierunek studiów	:	Informatyka algorytmiczna
Specjalność (jeśli dotyczy)	:	
Stopień studiów i forma	:	magisterskie, stacjonarne
Rodzaj przedmiotu	:	wybieralny
Kod przedmiotu	:	E2_W39
Grupa kursów	:	TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75	105			
Forma zaliczenia	zaliczenie				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	3	3			
w tym liczba odpowiadająca zajęciom o charakterze praktycznym (P)		3			
w tym liczba punktów odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	2	2			

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

CELE PRZEDMIOTU

C1 Przedstawienie podstawowych narzędzi algebraicznych używanych w kryptografii z kluczem publicznym.

C2 Utrwalenie wiedzy z wykładu, wyrobienie podstawowych intuicji.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy studenta:

W1 Zna podstawy arytmetyki ciał skończonych.

W2 Rozumie metodę sita ciał liczbowych.

W3 Rozumie algorytm Pohliga-Hellmana.

W4 Zna podstawy arytmetyki krzywych eliptycznych.

W5 Rozumie związki pomiędzy algorytmem LLL a algorytmem znajdowania NWD.

Z zakresu umiejętności studenta:

U1 Umie określić wymagania pomocne w wyborze bibliotek programistycznych w celu implementacji algorytmów kryptograficznych.

U2 Potrafi unikać podstawowych błędów w wyborze kluczy publicznych.

U3 Potrafi zaimplementować arytmetyke krzywych eliptycznych.

Z zakresu kompetencji społecznych studenta:

K1 Jest przygotowany do zdobywania nowych kompetencji i współpracy z fachowcami z innych dziedzin, zwłaszcza w zakresie wydajności i bezpieczeństwa projektowanych systemów informacyjnych.

K2 Potrafi wykonywać zadania w sposób pragmatyczny i kreatywny.

TREŚCI PROGRAMOWE

Forma zajęć - wykłady		
Wy1	Podstawowe twierdzenia użyte w trakcie kursu.	3h
Wy2	Ciała skończone.	3h
Wy3	Problem faktoryzacji modułów RSA n.	4h
Wy4	Problem logarytmu dyskretnego i podstawowe metody atakowania tego problemu.	5h
Wy5	Krzywe eliptyczne.	10h
Wy6	Kraty. Algorytm Lenstra-Lenstra-Lovasz.	5h

Forma zajęć - ćwiczenia		
Ćw1	Podstawowe twierdzenia użyte w trakcie kursu.	3h
Ćw2	Ciała skończone.	3h
Ćw3	Faktoryzacja liczb RSA.	4h
Ćw4	Problem Logarytmu Dyskretnego.	6h
Ćw5	Krzywe eliptyczne.	10h
Ćw6	Algorytm LLL.	4h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

1. Wykład tradycyjny
2. Rozwiązywanie zadań i problemów
3. Rozwiązywanie zadań programistycznych
4. Konsultacje
5. Praca własna studentów

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny	Numer efektu kształcenia	Sposób oceny efektu kształcenia
F1	W1-W5, K1-K2	Test końcowy.
F2	U1-U3, K1-K2	Ocena zadań związanych z implementacją.
P=50%*F1+50%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. Neal Koblitz: A Course in Number Theory and Cryptography, Springer, Graduate Texts in Mathematics Series
2. Joachim von zur Gathen, Jurgen Gerhard: Modern Computer Algebra, wyd.3 Cambridge University Press New York, NY, USA 2013

OPIEKUN PRZEDMIOTU

dr Przemysław Kubiak

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Algebraiczne aspekty kryptografii
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU INFORMATYKA ALGORYTMICZNA

Przedmiotowy efekt kształcenia	Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)	Cele przedmiotu**	Treści programowe**	Numer narzędzia dydaktycznego**
W1	K2_W01 K2_W02	C1	Wy1-Wy6	1 4 5
W2	K2_W01 K2_W02	C1	Wy1-Wy6	1 4 5
W3	K2_W03 K2_W04	C1	Wy1-Wy6	1 4 5
W4	K2_W03 K2_W04	C1	Wy1-Wy6	1 4 5
W5	K2_W03 K2_W04	C1	Wy1-Wy6	1 4 5
U1	K2_U03 K2_U05	C2	Ćw1-Ćw6	2 3 4 5
U2	K2_U02 K2_U05	C2	Ćw1-Ćw6	2 3 4 5
U3	K2_U01 K2_U03	C2	Ćw1-Ćw6	2 3 4 5
K1	K2_K03 K2_K10	C1 C2	Wy1-Wy6 Ćw1-Ćw6	1 2 3 4 5
K2	K2_K03 K2_K10	C1 C2	Wy1-Wy6 Ćw1-Ćw6	1 2 3 4 5