

WYDZIAŁ PODSTAWOWYCH PROBLEMÓW TECHNIKI
KARTA PRZEDMIOTU

Nazwa w języku polskim	:	Kryptografia
Nazwa w języku angielskim	:	Cryptography
Kierunek studiów	:	Informatyka algorytmiczna
Specjalność (jeśli dotyczy)	:	
Stopień studiów i forma	:	inżynierskie, stacjonarne
Rodzaj przedmiotu	:	wybieralny
Kod przedmiotu	:	E1_W35
Grupa kursów	:	TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	90	90			
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)	3	3			

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI
Algebra. Techniki kodowania. Elementarne prawdopodobieństwo, notacja duże-O, arytmetyka modularna.

CELE PRZEDMIOTU

- C1** Słuchacze poznają matematyczne i algorytmiczne podstawy współczesnej kryptografii
C2 Opanowanie technik i narzędzi matematycznych wykorzystywanych w kryptografii

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy studenta:

- W1** Zna metody zapewniające poufność komunikacji
W2 Zna metody zapewniające integralność komunikacji

Z zakresu umiejętności studenta:

- U1** Potrafi dobrać i wykorzystać narzędzia kryptograficzne
U2 Potrafi projektować bezpieczne protokoły

Z zakresu kompetencji społecznych studenta:

- K1** Rozumie konieczność stosowania technik kryptograficznych

TREŚCI PROGRAMOWE		
Forma zajęć - wykłady		
Wy1	Wstęp do kryptografii	2h
Wy2	One time pad. Szyfry strumieniowe	4h
Wy3	Szyfry blokowe	4h
Wy4	Ataki na szyfry blokowe	2h
Wy5	Integralność wiadomości. Funkcje haszujące.	2h
Wy6	Kryptografia nad liczbami pierwszymi	2h
Wy7	Kryptografia nad liczbami złożonymi	2h
Wy8	Infrastruktura klucza publicznego	2h
Wy9	Dowody z wiedzą zerową	2h
Wy10	Protokoły identyfikacji	2h
Wy11	Podpisy cyfrowe, zobowiązania	2h
Wy12	Dzielenie sekretu, oblivious transfer	2h
Wy13	Kryptografia nad krzywymi eliptycznymi	2h
Forma zajęć - ćwiczenia		
Ćw1	Rozwiązywanie problemów kryptograficznych	30h
STOSOWANE NARZĘDZIA DYDAKTYCZNE		
<ol style="list-style-type: none"> 1. Wykład tradycyjny 2. Rozwiązywanie zadań i problemów 3. Konsultacje 4. Praca własna studentów 		
OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA		
Oceny	Numer efektu kształcenia	Sposób oceny efektu kształcenia
F1	W1-W2, K1-K1	Kolokwium
F2	U1-U2, K1-K1	Listy ćwiczeń
P=60%*F1+40%*F2		
LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA		
<ol style="list-style-type: none"> 1. Introduction to modern cryptography - Jonathan Katz, Yehuda Lindell 2. Kryptografia w teorii i praktyce - Douglas R. Stinson 3. Lecture Notes on Cryptography - S. GoldwasserM. Bellare 		
OPIEKUN PRZEDMIOTU		
dr Filip Zagórski		

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Kryptografia

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	K1_W01 K1_W09	C1	Wy1-Wy13	1 3 4
W2	K1_W01 K1_W03 K1_W04 K1_W05 K1_W06 K1_W09 K1_W11	C1	Wy1-Wy13	1 3 4
U1	K1_U01 K1_U02 K1_U03 K1_U06 K1_U09 K1_U10 K1_U11 K1_U15 K1_U25 K1_U30 K1_U31	C2	Ćw1-Ćw1	2 3 4
U2	K1_U01 K1_U03 K1_U19 K1_U25 K1_U28 K1_U31	C2	Ćw1-Ćw1	2 3 4
K1	K1_K04 K1_K10	C1 C2	Wy1-Wy13 Ćw1-Ćw1	1 2 3 4