WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim : **Kryptografia**
Nazwa przedmiotu w języku angielskim : **Cryptography**
Kierunek studiów : **Informatyka algorytmiczna**
Specjalność (jeśli dotyczy) : **—**
Poziom i forma studiów : **I stopień, stacjonarna**
Rodzaj przedmiotu : **wybieralny**
Kod przedmiotu : **INP002310Wc**
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 punktów odpowiadająca zajęciom o charakterze praktycznym (P)		3			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2	2			

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

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 - wykład		
Wy1	Wstęp do kryptografii	2h
Wy2	One time pad. Szyfry strumieniowe	4h
Wy3	Szyfry blokowe, kryptografia symetryczna	4h
Wy4	Ataki na kryptografię symetryczną	2h
Wy5	Funkcje haszujące i ich zastosowania	2h
Wy6	RSA, szyfrowanie asymetryczne, podpisy cyfrowe	2h
Wy7	Kryptografia asymetryczna oparta na problemie DLP	2h
Wy8	Infrastruktura klucza publicznego	2h
Wy9	Bezpieczna komunikacja	2h
Wy10	Protokoły identyfikacji i uwierzytelniania	2h
Wy11	Dowody z wiedzą zerową	2h
Wy12	Dzielenie sekretu, oblivious transfer	2h
Wy13	Przestępczość związana z kryptografią	2h
	Suma godzin	30h

Forma zajęć - ćwiczenia		
Ćw1	Rozwiązywanie problemów kryptograficznych	30h
	Suma godzin	30h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

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

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F - formatująca (w trakcie semestru), P - podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	W1-W2, K1-K1	Kolokwium
F2	U1-U2, K1-K1	Listy ćwiczeń
P=60%*F1+40%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. Lecture Notes on Introduction to Cryptography, CMU, Vipul Goyal, dostępne online
2. Kryptografia w teorii i praktyce - Douglas R. Stinson
3. Lecture Notes on Cryptography - S. GoldwasserM. Bellare, dostępne online
4. Handbook of Applied Cryptography, Paul C. van Oorschot , Scott A. Vanstone A. J. Menezes, dostępne online

OPIEKUN PRZEDMIOTU
prof. Mirosław Kutyłowski

MACIERZ POWIĄZANIA EFEKTÓW UCZENIA SIĘ DLA PRZEDMIOTU

Kryptografia

Z EFEKTAMI UCZENIA SIĘ NA KIERUNKU INFORMATYKA ALGORYTMICZNA

Przedmiotowy efekt uczenia się	Odniesienie przedmiotowego efektu do efektów uczenia się 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 4 5
W2	K1_W01 K1_W03 K1_W04 K1_W05 K1_W06 K1_W09 K1_W11	C1	Wy1-Wy13	1 4 5
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 5
U2	K1_U01 K1_U03 K1_U19 K1_U25 K1_U28 K1_U31	C2	Ćw1-Ćw1	2 3 4 5
K1	K1_K04 K1_K13	C1 C2	Wy1-Wy13 Ćw1-Ćw1	1 2 3 4 5