Zał nr 4 do ZW

WYDZIAŁ PODSTAWOWYCH PROBLEMÓW TECHNIKI

KARTA PRZEDMIOTU

Nazwa w języku polskim	:	**Kryptografia i Bezpieczeństwo Komputerowe**
Nazwa w języku angielskim	:	**Cryptography and Computer Security**
Kierunek studiów	:	Informatyka
Specjalność (jeśli dotyczy)	:	
Stopień studiów i forma	:	inżynierskie, stacjonarne
Rodzaj przedmiotu	:	wybieralny
Kod przedmiotu	:	E1_W23
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 podstawy zagadnień współczesnej kryptografii i bezpieczeństwa komputerowego.

C2 Opanowanie technik kryptograficznych służączych zabezpieczaniu danych.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy studenta:

W1 Zna metody zapewniające poufność komunikacji

W2 Zna metody zapewniające integralność

Z zakresu umiejętności studenta:

U1 Potrafi wykorzystywać narzędzia kryptograficzne

U2 Potrafi budować bezpieczne aplikacje i systemy

Z zakresu kompetencji społecznych studenta:

K1 Rozumie konieczność stosowania technik kryptograficznych

K2 Potrafi dobrać adekwatne narzędzia w celu tworzenia bezpiecznych aplikacji

TREŚCI PROGRAMOWE		
Forma zajęć - wykłady		
Wy1	Pojęcie systemu kryptograficznego	2h
Wy2	One time pad. Szyfry strumieniowe	2h
Wy3	Szyfry blokowe	2h
Wy4	Ataki na szyfry blokowe	2h
Wy5	Integralność wiadomości. Funkcje haszujące.	3h
Wy6	Kryptografia nad liczbami pierwszymi	3h
Wy7	Kryptografia nad liczbami złożonymi	2h
Wy8	Infrastruktura klucza publicznego	2h
Wy9	Protokoły identyfikacji	2h
Wy10	Prywatność	2h
Wy11	Dzielenie sekretu	2h
Wy12	Urządzenia kryptograficzne	2h
Wy13	Bezpieczny kod?	4h
Forma zajęć - laboratorium		
Lab1	PGP	2h
Lab2	Sesje w aplikacjach webowych	4h
Lab3	Ataki na aplikacje webowe	4h
Lab4	SSL	2h
Lab5	Implementacja wybranego kryptosystemu	2h
Lab6	Wykorzystanie bibliotek kryptograficznych	2h
Lab7	Bezpieczeństwo baz danych	2h
Lab8	Bezpieczne aplikacje	4h
Lab9	Implementacja wybranych protokołów kryptograficznych	4h
Lab10	Wirusy. Cracking.	4h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

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

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny	Numer efektu kształcenia	Sposób oceny efektu kształcenia
F1	W1-W2, K1-K2	Egzamin
F2	U1-U2, K1-K2	Listy zadań programistycznych
P=60%*F1+40%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
1. Introduction to modern cryptography - Jonathan Katz, Yehuda Lindell 2. Kryptografia w teorii i praktyce - Douglas R. Stinson 3. The Art of Software Security Assessment – Identifying and Preventing Software Vulnerabilities - Mark Dowd, John McDonald, Justin Schuh
OPIEKUN PRZEDMIOTU
dr Filip Zagórski

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Kryptografia i Bezpieczeństwo Komputerowe
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU INFORMATYKA

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 2 5
W2	K1_W01 K1_W03 K1_W04 K1_W05 K1_W06 K1_W09 K1_W14	C1	Wy1-Wy13	1 2 5
U1	K1_U01 K1_U02 K1_U03 K1_U12 K1_U13 K1_U15 K1_U17 K1_U25 K1_U30 K1_U32	C1	Lab1-Lab10	3 4 5
U2	K1_U12 K1_U13 K1_U15 K1_U25 K1_U32	C1	Lab1-Lab10	3 4 5
K1	K1_K04 K1_K13	C1 C2	Wy1-Wy13 Lab1-Lab10	1 2 3 4 5
K2	K1_K03 K1_K04 K1_K05 K1_K10 K1_K11 K1_K13	C1 C2	Wy1-Wy13 Lab1-Lab10	1 2 3 4 5