

WYDZIAŁ PODSTAWOWYCH PROBLEMÓW TECHNIKI						
KARTA PRZEDMIOTU						
Nazwa w języku polskim	:	Kryptografia				
Nazwa w języku angielskim	:	Cryptography				
Kierunek studiów	:	Informatyka				
Specjalność (jeśli dotyczy)	:					
Stopień studiów i forma	:	magisterskie, stacjonarne				
Rodzaj przedmiotu	:	obowiązkowy				
Kod przedmiotu	:	E2_I03				
Grupa kursów	:	TAK				
		Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)		30	30	30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)		45	45	60		
Forma zaliczenia		egzamin				
Dla grupy kursów zaznaczyć kurs końcowy		X				
Liczba punktów ECTS		1	2	2		
w tym liczba odpowiadająca zajęciom o charakterze praktycznym (P)			2	2		
w tym liczba punktów odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)		1	2	2		
<p>WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI standardowa znajomość zagadnień z zakresu: algebra abstrakcyjna, algorytmy i struktury danych, rachunek prawdopodobieństwa, złożoność obliczeniowa.</p>						
<p align="center">CELE PRZEDMIOTU</p> <p>C1 prezentacja zaawansowanych technik kryptograficznych stosowanych w praktyce</p> <p>C2 zrozumienie zaawansowanych mechanizmów współczesnej kryptografii</p> <p>C3 zdobycie umiejętności w implementacji technik kryptograficznych</p>						

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy studenta:

- W1** zna najważniejsze techniki współczesnej kryptografii służące zapewnieniu bezpieczeństwa
- W2** zna narzędzia i struktury matematyczne służące do konstrukcji schematów kryptograficznych
- W3** zna najważniejsze problemy i wyzwania stojące przed kryptografią i kryptoanalizą

Z zakresu umiejętności studenta:

- U1** potrafi budować narzędzia kryptograficzne służące zapewnieniu bezpieczeństwa
- U2** potrafi budować i wykorzystywać narzędzia kryptoanalityczne
- U3** potrafi posługiwać się abstrakcyjnymi strukturami matematycznymi służącymi do implementacji systemów kryptograficznych
- U4** potrafi ocenić systemy kryptograficzne i dokonywać wyboru rozwiązań pod kątem postawionych wymagań

Z zakresu kompetencji społecznych studenta:

- K1** rozumie konieczność stosowania technik kryptograficznych
- K2** potrafi dostosować rozwiązania kryptograficzne do uwarunkowań wynikających z zachowania użytkowników
- K3** potrafi dostosować rozwiązania kryptograficzne do uwarunkowań ekonomicznych i wymagań prawnych
- K4** potrafi oszacować praktyczny wymiar ataków i zagrożeń

TREŚCI PROGRAMOWE

Forma zajęć - wykłady		
Wy1	Kryptografia	2h
Wy2	One time pad. Szyfry strumieniowe	2h
Wy3	Szyfry blokowe	2h
Wy4	Abstrakcje blokowych schematów szyfrowania	2h
Wy5	Integralność wiadomości. Funkcje haszujące.	3h
Wy6	Bezpieczeństwo względem ataków aktywnych.	2h
Wy7	Problem logarytmu dyskretnego	2h
Wy8	Kryptografia nad liczbami złożonymi	2h
Wy9	Bezpieczeństwo kryptosystemów klucza publicznego.	2h
Wy10	Podpisy cyfrowe	2h
Wy11	Kryptosystemy klucza publicznego a wyrocznie losowe	2h
Wy12	Dowody z wiedzą zerową	2h
Wy13	Bezpieczne protokoły	2h
Wy14	Nieklasyczne techniki kryptograficzne	3h

Forma zajęć - ćwiczenia		
Ćw1	Ataki ciphertext-only	2h
Ćw2	Tajność doskonała	2h
Ćw3	Ataki na szyfry blokowe	2h
Ćw4	Tryby szyfrowania	2h
Ćw5	Funkcje haszujące, MAC	2h
Ćw6	CPA i CCA	2h
Ćw7	Protokoły uzgadniania kluczy. ElGamal	2h
Ćw8	RSA	2h
Ćw9	Logarytm dyskretny, faktoryzacja	2h
Ćw10	Podpisy cyfrowe	2h
Ćw11	Wyrocznie	2h
Ćw12	Dowody interaktywne	2h
Ćw13	Oblivious transfer	2h
Ćw14	Kryptografia kwantowa	2h
Forma zajęć - laboratorium		
Lab1	Implementacja providerów kryptograficznych	2h
Lab2	Zabezpieczanie danych	4h
Lab3	Funkcje haszujące	4h
Lab4	Testy pierwszości	4h
Lab5	Dyskretny logarytm	4h
Lab6	Faktoryzacja	4h
Lab7	Implementacja wybranego schematu podpisu	6h
STOSOWANE NARZĘDZIA DYDAKTYCZNE		
<ol style="list-style-type: none"> 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-W3, K1-K4	Egzamin
F2	U1-U4, K1-K4	kartkówki, zadania do wykonania samodzielnie przez studentów
F3	U1-U4, K1-K4	odbiór zadań programistycznych
$P=40\%*F1+30\%*F2+30\%*F3$		
LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA		
<ol style="list-style-type: none"> 1. Introduction to modern cryptography. Jonathan Katz, Yehuda Lindell, ISBN: 1584885513 2. Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, ISBN:0-8493-8523-7 		

OPIEKUN PRZEDMIOTU

dr Filip Zagórski

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Kryptografia
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	K2_W01 K2_W02 K2_W03_B K2_W04_B	C1	Wy1-Wy14	1 4 5
W2	K2_W01 K2_W02 K2_W03_B K2_W04_B K2_W05	C1	Wy1-Wy14	1 4 5
W3	K2_W01 K2_W02 K2_W03_B K2_W04_B K2_W05	C1	Wy1-Wy14	1 4 5
U1	K2_U01_B K2_U16 K2_U19_B K2_U21_B	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U2	K2_U01_B K2_U08_B K2_U12_B K2_U14 K2_U18_B K2_U19_B K2_U21_B K2_U22_B	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U3	K2_U01_B K2_U09_B K2_U12_B	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U4	K2_U01_B K2_U05_B K2_U08_B K2_U09_A K2_U10 K2_U12_B K2_U13 K2_U14 K2_U15 K2_U16 K2_U17 K2_U18_B K2_U19_B K2_U20 K2_U21_B	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
K1	K2_K01_B K2_K02 K2_K03 K2_K04 K2_K11 K2_K12 K2_K13 K2_K14_B K2_K15 K2_K16	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K2	K2_K01_B K2_K02 K2_K03 K2_K04 K2_K05 K2_K10 K2_K13 K2_K14_B K2_K15 K2_K16	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K3	K2_K04	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K4	K2_K01_B K2_K03 K2_K04 K2_K05 K2_K10 K2_K12 K2_K13 K2_K14_B K2_K15 K2_K16	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5