WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI/KATEDRA PODSTAW INFORMATYKI

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 : **II stopień, stacjonarna**
Rodzaj przedmiotu : **obowiązkowy**
Kod przedmiotu : W04INA-SM0008G
Grupa kursów : **TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30	15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	45	60	45		
Forma zaliczenia	egzamin				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	2	2	1		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		2	1		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2	2	1		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

standardowa znajomość zagadnień z zakresu: algebra abstrakcyjna, algorytmy i struktury danych, rachunek prawdopodobieństwa, złożoność obliczeniowa.

CELE PRZEDMIOTU

C1 prezentacja zaawansowanych technik kryptograficznych stosowanych w praktyce

C2 zrozumienie zaawansowanych mechanizmów współczesnej kryptografii

C3 zdobycie umiejętności w implementacji technik kryptograficznych

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 dostosowań rozwiązania kryptograficzne do uwarunkowań ekonomicznych i wymagań prawnych

K4 potrafi oszacować praktyczny wymiar ataków i zagrożeń

TREŚCI PROGRAMOWE

Forma zajęć - wykład		
Wy1	Kryptografia - historia	2h
Wy2	One time pad. Szyfry strumieniowe	2h
Wy3	Szyfry blokowe	2h
Wy4	Abstrakcje blokowych schematów szyfrowania	2h
Wy5	Integralność wiadomości. Funkcje haszujące.	2h
Wy6	Bezpieczeństwo względem ataków aktywnych.	2h
Wy7	Problem logarytmu dyskretnego	2h
Wy8	Kryptografia nad liczbami złożonymi	2h
Wy9	Podpisy cyfrowe	2h
Wy10	Bezpieczne obliczenia wielostronne. Oblivious transfer	2h
Wy11	Dowody z wiedzą zerową	2h
Wy12	Zobowiązania bitowe, weryfiowalne współdzielenie serkretów	2h
Wy13	Kryptografia kwantowa	2h
Wy14	Schematy kryptograficzne odporne na kwantowego adwersarza	4h
	Suma godzin	30h

Forma zajęć - ćwiczenia		
Ćw1	Tajność doskonała. Ataki ciphertext-only	2h
Ćw2	Ataki na szyfry blokowe	2h
Ćw3	Ataki na szyfry strumieniowe. Własności generatorów pseudolosowych.	2h
Ćw4	Funkcje haszujące, MAC. Własności funkcji pseudolosowych.	2h
Ćw5	Attacks on RSA. Faktoryzacja.	2h
Ćw6	Protokoły uzgadniania kluczy. ElGamal. Problem dyskretnego logarytmu	2h
Ćw7	CPA i CCA	2h
Ćw8	Ataki czasowe na implementacje RSA	2h
Ćw9	Oblivious transfer	2h
Ćw10	Dowody interaktywne. Dowody z wiedzą zerową	4h
Ćw11	Homomorphic encryption	2h
Ćw12	Obliczenia na zaszyfrowanych danych	2h
Ćw13	Kryptografia kwantowa	2h
Ćw14	Kryptografia post-kwantowa	2h
	Suma godzin	30h

Forma zajęć - laboratorium		
Lab1	Implementacja providerów kryptograficznych	2h
Lab2	Zabezpieczanie danych	2h
Lab3	Funkcje haszujące	2h
Lab4	Testy pierwszości	2h
Lab5	Dyskretny logarytm	2h
Lab6	Faktoryzacja	2h
Lab7	Implementacja wybranego schematu podpisu	3h
	Suma godzin	15h

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 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-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

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
3. Cryptography. Theory and practice - Douglas R. Stinson
4. The Foundations of Cryptography (https://www.wisdom.weizmann.ac.il/ oded/foc-drafts.html) - Oded Goldreich
5. Lecture Notes on Cryptography (https://cseweb.ucsd.edu/ mihir/papers/gb.pdf) - S. Goldwasser, M. Bellare

OPIEKUN PRZEDMIOTU

dr Filip Zagórski

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	Cele przedmiotu**	Treści programowe**	Numer narzędzia dydaktycznego**
W1	K2_W01 K2_W02 K2_W03 K2_W04	C1	Wy1-Wy14	1 4 5
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W07 K2_W08	C1	Wy1-Wy14	1 4 5
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08	C1	Wy1-Wy14	1 4 5
U1	K2_U05 K2_U06 K2_U10 K2_U12	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U2	K2_U01 K2_U03 K2_U04 K2_U05 K2_U06 K2_U12 K2_U13	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U3	K2_U03 K2_U06	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U4	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U11 K2_U12	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
K1	K2_K02 K2_K03 K2_K05 K2_K07 K2_K09 K2_K10	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K2	K2_K02 K2_K03 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K3	K2_K01 K2_K05 K2_K09 K2_K12	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K4	K2_K01 K2_K02 K2_K03 K2_K05 K2_K07 K2_K09 K2_K10	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5