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**
Język wykładowy : **polski**
Cykl kształcenia od : **2023/2024**
Kod przedmiotu : **W04INA-SM0015G**
Grupa zajęć : **TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30	15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	50	50		
Forma zaliczenia	egzamin				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	2	2	2		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		4			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	3.64				

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 UCZENIA SIĘ

Z zakresu wiedzy studenta:

W1 Zna najważniejsze techniki współczesnej kryptografii służące zapewnieniu bezpieczeństwa systemów IT.

W2 Zna narzędzia i struktury matematyczne wykorzystywane do konstrukcji schematów kryptograficznych.

W3 Zna najważniejsze problemy i wyzwania stojące przed kryptografią i kryptoanalizą.

Z zakresu umiejętności studenta:

U1 Potrafi budować systemy kryptograficzne do zapewnienia bezpieczeństwa systemów IT.

U2 Potrafi posługiwać się abstrakcyjnymi strukturami matematycznymi do analizy i implementacji systemów kryptograficznych.

U3 Potrafi oceniać systemy kryptograficzne i dokonywać wyboru rozwiązań dla postawionych wymagań.

Z zakresu kompetencji społecznych studenta:

K1 Rozumie konieczność stosowania technik kryptograficznych.

K2 Potrafi dostosować rozwiązania kryptograficzne do uwarunkowań.

K3 Potrafi oszacować praktyczny wymiar ataków i zagrożeń.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		
Wy1	Kryptografia – historia.	2h
Wy2	Systemy z kluczem symetrycznym – wstęp, modele bezpieczeństwa.	2h
Wy3	One time pad. Szyfry strumieniowe.	2h
Wy4	Szyfry blokowe.	2h
Wy5	Integralność wiadomości. Funkcje haszujące.	2h
Wy6	Systemy z kluczem publicznym – wstęp, modele bezpieczeństwa.	2h
Wy7	Dowody z wiedzą zerową.	2h
Wy8	Schematy identyfikacji.	2h
Wy9	Podpisy cyfrowe.	2h
Wy10	Protokoły ustalania kluczy.	2h
Wy11	Anonimowość i zaprzeczalność.	2h
Wy12	Bezpieczne obliczenia wielostronne. Oblivious transfer.	2h
Wy13	Współdzielenie sekretów. Szyfrowane rozgłaszanie z wykluczaniem.	2h
Wy14	Zobowiązania. Reszyfrowanie.	2h
Wy15	Kryptografia kwantowa i postkwantowa.	2h
	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.	3h
Ćw5	Schematy identyfikacji. Ataki.	3h
Ćw6	Schematy podpisu. Ataki.	3h
Ćw7	Schematy ustalania kluczy symetrycznych. Ataki.	3h
Ćw8	Schematy szyfrowania z kluczem publicznym. Ataki.	3h
Ćw9	Anonimowość. Ataki.	3h
Ćw10	Zaprzeczalność wykonywania schematów i protokołów kryptograficznych.	3h
Ćw11	Współdzielenie sekretów. Szyfrowane rozgłaszanie. Ataki.	3h
	Suma godzin	30h

Forma zajęć - laboratorium		
Lab1	Zabezpieczanie danych.	3h
Lab2	Realizacja wybranych ataków.	3h
Lab3	Implementacja wybranego schematu identyfikacji.	3h
Lab4	Implementacja wybranego schematu podpisu.	3h
Lab5	Implementacja wybranego schematu ustalania kluczy.	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-K3	Egzamin
F2	U1-U3, K1-K3	Listy zadań do samodzielnego rozwiązania.
F3	U1-U3, K1-K3	Listy zagadnień do samodzielnej implementacji.
P=50%*F1+25%*F2+25%*F3		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. Lecture Notes on Cryptography (https://cseweb.ucsd.edu/mihir/papers/gb.pdf) - S. Goldwasser, M. Bellare.
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.html) - Oded Goldreich.
5. Introduction to modern cryptography. Jonathan Katz, Yehuda Lindell, ISBN: 1584885513.

NAUCZYCIEL AKADEMICKI ODPOWIEDZIALNY ZA PRZEDMIOT

dr hab. inż. Łukasz Krzywiecki

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-Wy15	1 4 5
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W07 K2_W08	C1	Wy1-Wy15	1 4 5
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08	C1	Wy1-Wy15	1 4 5
U1	K2_U05 K2_U06 K2_U12 K2_U13	C2 C3	Ćw1-Ćw11 Lab1-Lab5	2 3 4 5
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U12 K2_U13	C2 C3	Ćw1-Ćw11 Lab1-Lab5	2 3 4 5
U3	K2_U01 K2_U02 K2_U12	C2 C3	Ćw1-Ćw11 Lab1-Lab5	2 3 4 5
K1	K2_K02 K2_K03 K2_K05 K2_K10	C1 C2 C3	Wy1-Wy15 Ćw1-Ćw11 Lab1-Lab5	1 2 3 4 5
K2	K2_K02 K2_K03 K2_K06 K2_K08 K2_K10	C1 C2 C3	Wy1-Wy15 Ćw1-Ćw11 Lab1-Lab5	1 2 3 4 5
K3	K2_K01 K2_K02 K2_K03 K2_K05 K2_K07 K2_K08 K2_K10	C1 C2 C3	Wy1-Wy15 Ćw1-Ćw11 Lab1-Lab5	1 2 3 4 5