WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ I ZARZĄDZANIA WIT
POD AUSPICJAMI POLSKIEJ AKADEMII NAUK
01-447 Warszawa \ ul. Newelska 6 \ www.WIT.edu.pl

WYDZIAŁ INFORMATYKI

Kierunek studiów	Informatyka
Profil	Praktyczny
Stopień studiów	1-go stopnia
Forma studiów	stacjonarne

Sylabus przedmiotu

Systemy kryptograficzne

1. Dane podstawowe

Status programowy przedmiotu	Blok A: Bezpieczeństwo informacji
Rodzaj przedmiotu	Obligatoryjny
Kod przedmiotu	ID-SKR-DR
Rok studiów	3
Semestr	6
Osoba odpowiedzialna za przedmiot	dr inż. Piotr Mroczkowski
Język wykładowy	polski

2. Wymiar godzin i forma zajęć

Rodzaj	Liczba godzin
Wykład	15
Ćwiczenia	15
Laboratorium	8
Razem godzin	38

3. Cele przedmiotu

Kod	Cel
CP1	Zapoznanie studentów z wybranymi systemami kryptograficznymi.
CP2	Zapoznanie studentów z zastosowaniem kryptografii asymetrycznej w ochronie informacji.
CP3	Zapoznanie studentów ze współczesnymi algorytmami klucza publicznego.
CP4	Zapoznanie studentów ze współczesnymi protokołami kryptografiocznymi.
CP5	Poznanie komercyjnych zastosowań kryptografii.

4. Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

Student na wiedzę w zakresie przedmiotu Wstęp do Kryptologii.

5. Efekty uczenia się

Wiedza

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W1	Zna i rozumie współczesne systemy kryptograficzne.	CP1, CP2, CP3, CP4	IK6_W14
EU-W2	Zna i rozumie ideę kryptografii asymetrycznej.	CP2, CP3	IK6_W14
EU-W3	Zna i rozumie usługi kryptograficzne realizowane za pomocą kryptosystemów asymetrycznych.	CP2, CP3, CP4	IK6_W14
EU-W4	Zna i rozumie algorytmy klucza publicznego oraz ich bezpieczeństwo.	CP3, CP4	IK6_W14
EU-W5	Zna i rozumie potrzebę wykorzystania kryptografii asymetrycznej w zastosowaniach komercyjnych.	CP1, CP5	IK6_W14

Umiejętności

Kod	Student potrafi:	Realizuje cel	Efekty kierunkowe
EU-U1	Potrafi opisać znaczenie kryptografii asymetrycznej do ochrony informacji.	CP1, CP2	IK6_U03, IK6_U14
EU-U2	Potrafi opracować podstawowy protokół kryptograficznej ochrony informacji.	CP2, CP3, CP4	IK6_U14
EU-U3	Potrafi wykorzystać współczesne algorytmy klucza publicznego w systemach kryptograficznych.	CP2, CP3, CP4, CP5	IK6_U14
EU-U4	Potrafi opisać znaczenie kryptografii w zastosowaniach komercyjnych.	CP1, CP4, CP5	IK6_U14

Kompetencje

Kod	Student jest gotów do:	Realizuje cel	Efekty kierunkowe
EU-K1	Jest gotów do zaprojektowania protokołu kryptograficznego ochrony informacji.	CP1, CP2, CP3, CP4, CP5	IK6_K01, IK6_K03
EU-K2	Jest gotów do zapewnienia bezpieczeństwa informacji w systemach kryptograficznych.	CP1, CP2, CP3, CP4, CP5	IK6_K01, IK6_K03

6. Treści programowe

Kod	Tematyka	wykład	ćwiczenia	laboratorium	Realizuje efekt
TP1	Wprowadzenie do przedmiotu – omówienie podstawowych pojęć i definicji z dziedziny systemów kryptograficznych. Wprowadzenie do kryptologii klucza publicznego. Idea szyfrowania/deszyfrowania asymetrycznego. Idea generacji/weryfikacji podpisu cyfrowego. Idea wykorzystania problemów trudno obliczeniowych wykorzystywanych w kryptografii asymetrycznej.	3	0	0	EU-U1, EU-W2, EU-W3
TP2	Generator grupy multiplikatywnej. Algorytm Diffiego-Hellmana oraz rozszerzony algorytm Diffiego-Hellmana. Bezpieczeństwo algorytmu Diffiego-Hellmana. Atak metodą „man in the middle" na algorytm Diffiego-Hellmana.	3	3	2	EU-K1, EU-K2, EU-U2, EU-W1
TP3	Kryptosystem asymetryczny RSA. Omówienie problemu faktoryzacji liczb złożonych oraz problemu RSA. Szczegółowe omówienie algorytmów: generacji kluczy, szyfrowania i deszyfrowania, generacji i weryfikacji podpisów cyfrowych RSA. Omówienie zagadnień związanych z bezpieczeństwem kryptosystemu RSA.	3	6	3	EU-K1, EU-K2, EU-U2, EU-U3, EU-W1, EU-W2, EU-W3, EU-W4
TP4	Kryptosystem asymetryczny ElGamala. Omówienie problemu obliczania logarytmów dyskretnych w ciałach skończonych. Szczegółowe omówienie algorytmów: generacji kluczy, szyfrowania i deszyfrowania, generacji i weryfikacji podpisów cyfrowych ElGamala. Omówienie zagadnień związanych z bezpieczeństwem kryptosystemu ElGamala.	3	6	3	EU-K1, EU-K2, EU-U1, EU-U2, EU-U3, EU-W1, EU-W2, EU-W3, EU-W4

Kod	Tematyka	wykład	ćwiczenia	laboratorium	Realizuje efekt
TP5	Omówienie wybranego systemu kryptograficznego.	3	0	0	EU-K1, EU-K2, EU-U2, EU-U3, EU-U4, EU-W1, EU-W2, EU-W3, EU-W4, EU-W5

Razem godzin: 38

7. Metody kształcenia

Kod	Metoda
MK1	Wykład wsparty prezentacją komputerową.
MK2	Praca ze źródłami literaturowymi.
MK3	Rozwiązywanie zadań pod nadzorem prowadzącego.
MK4	Krótkie sprawdzany pisemne z wiedzy teoretycznej (opcjonalnie).
MK5	Projekt realizowany na zajęciach laboratoryjnych.
MK6	Sprawozdanie pisemne z laboratorium.

8. Nakład pracy studenta

Aktywność studenta	Obciążenie
Przygotowanie do ćwiczeń.	10
Przygotowanie do egzaminu.	15
Przygotowanie do kolokwium.	10
Przygotowanie do laboratorium.	6
Przygotowanie do wykładu.	5
Praca z nauczycielem związana z: ćwiczenia	15
Praca z nauczycielem związana z: laboratorium	8
Praca z nauczycielem związana z: wykład	15
Liczba punktów ECTS (1 punkt=25h)	3
Procentowy udział pracy własnej studenta w sumarycznym obciążeniu studenta	54,76%
Sumaryczne obciążenie pracą studenta	84

9. Status zaliczenia przedmiotu

Egzamin pisemny.

Forma studiów	Egzamin	Praca egzaminacyjna	Zaliczenie	Praca zaliczeniowa
stacjonarne	×			

10. Metody weryfikacji efektów uczenia się

Składowe oceny końcowej

Forma sprawdzenia	Wybrana forma	Punktacja	Realizuje efekt
Egzamin pisemny	×	50	EU-U4, EU-W5, EU-W3, EU-U1, EU-W4, EU-W2, EU-W1
Egzamin ustny			
Sprawdzian pisemny			
Zaliczeniowy przegląd prac			
Referat pisemny			
Referat ustny			
Kolokwium	×	30	EU-W5, EU-W3, EU-W4, EU-W2, EU-W1
Praca domowa			
Miniprojekt			
Praca na zajęciach			
Projekt z dokumentacją	×	20	EU-K2, EU-U3, EU-K1, EU-W3, EU-U2, EU-W4, EU-W2
Ustna prezentacja projektu			
Obecność na zajęciach			
Sprawdzian ustny			
Kartkówka			
Aktywność na zajęciach			
Egzaminacyjny przegląd prac			
Sprawozdanie z praktyki zawodowej			
Prezentacja indywidualna			
Prezentacja zespołowa			

Zasady wyliczania oceny z przedmiotu

Zakres punktów	Ocena
0 – 49	2,0
50 – 59	3,0
60 – 69	3,5
70 – 79	4,0
80 – 89	4,5
90 – 100	5,0

11. Macierz realizacji przedmiotu

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-W1	CP1, CP2, CP3, CP4	TP2, TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-W2	CP2, CP3	TP1, TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-W3	CP2, CP3, CP4	TP1, TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-W4	CP3, CP4	TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-W5	CP1, CP5	TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-U1	CP1, CP2	TP1, TP4	MK1, MK2, MK3, MK4, MK5, MK6
EU-U2	CP2, CP3, CP4	TP2, TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-U3	CP2, CP3, CP4, CP5	TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-U4	CP1, CP4, CP5	TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-K1	CP1, CP2, CP3, CP4, CP5	TP2, TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6
EU-K2	CP1, CP2, CP3, CP4, CP5	TP2, TP3, TP4, TP5	MK1, MK2, MK3, MK4, MK5, MK6

12. Odniesienie efektów uczenia się

Efekt uczenia się	Efekty kształcenia dla kierunku studiów	Charakterystyki drugiego stopnia w obszarze kształcenia
EU-W1	IK6_W14	P6S_WG
EU-W2	IK6_W14	P6S_WG
EU-W3	IK6_W14	P6S_WG
EU-W4	IK6_W14	P6S_WG
EU-W5	IK6_W14	P6S_WG
EU-U1	IK6_U14, IK6_U03	P6S_UU, P6S_UW
EU-U2	IK6_U14	P6S_UW
EU-U3	IK6_U14	P6S_UW
EU-U4	IK6_U14	P6S_UW
EU-K1	IK6_K03, IK6_K01	P6S_KK
EU-K2	IK6_K03, IK6_K01	P6S_KK

13. Literatura

Literatura podstawowa

1. Douglas Stinson, Kryptografia w teorii i praktyce, WNT, 2005
2. Janusz Szmidt, Wstęp do kryptologii, WSISiZ, 2004
3. Marcin Karbowski, Podstawy kryptografii, Helion, 2014

Literatura uzupełniająca

1. Jean-Philippe Aumasson, Nowiczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, PWN, 2017
2. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji., Helion, 2012

Strony WWW

1. Pakiet programowania funkcji matematycznych., sagemath.org

14. Informacje o nauczycielach akademickich

Osoby odpowiedzialne za przedmiot

1. dr inż. Piotr Mroczkowski

Osoby prowądzace przedmiot

1. dr inż. Piotr Mroczkowski