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	niestacjonarne

Sylabus przedmiotu

Wstęp do kryptologii

1. Dane podstawowe

Status programowy przedmiotu	Blok A: Bezpieczeństwo informacji
Rodzaj przedmiotu	Obligatoryjny
Kod przedmiotu	IZ-WKR-ZR
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	16
Ćwiczenia	16
Razem godzin	32

3. Cele przedmiotu

Kod	Cel
CP1	Zapoznanie studentów z zagadnieniami bezpieczeństwa informacji.
CP2	Zapoznanie studentów z zagadnieniami kryptologii i kryptoanalizy.
CP3	Zapoznanie studentów z usługami kryptograficznej ochrony informacji.
CP4	Poznanie podstawowych szyfrów klasycznych.
CP5	Poznanie współczesnych algorytmów kryptograficznych.

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

Znajomość zagadnień algebry, matematyki i matematyki dyskretnej.

5. Efekty uczenia się

Wiedza

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W1	Student zna i rozumie zagrożenia dla bezpieczeństwa informacji.	CP1	IK6_W14
EU-W2	Student zna i rozumie cele i zadania kryptologii.	CP1, CP2	IK6_W14
EU-W3	Student zna i rozumie podstawowe usługi kryptograficzne.	CP1, CP2, CP3	IK6_W14
EU-W4	Student zna i rozumie podstawowe szyfry klasyczne.	CP2, CP3, CP4	IK6_W14
EU-W5	Student zna i rozumie współczesne algorytmy kryptograficzne.	CP2, CP3, CP5	IK6_W14

Umiejętności

Kod	Student potrafi:	Realizuje cel	Efekty kierunkowe
EU-U1	Student potrafi definiować zagrożenia dla bezpieczeństwa informacji i im zapobiegać.	CP1	IK6_U14
EU-U2	Student potrafi zdefiniować cele i zadania kryptologii.	CP1, CP2	IK6_U14
EU-U3	Student potrafi posługiwać się szyframi klasycznymi.	CP2, CP3, CP4	IK6_U14
EU-U4	Student potrafi wykorzystać współczesne algorytmy kryptograficzne do zapewnienia usług kryptograficznej ochrony informacji.	CP3, CP5	IK6_U14
EU-U5	Student potrafi wykorzystać usługi kryptograficznej ochrony informacji do zapewnienia kryptograficznego bezpieczeństwa informacji.	CP1, CP2, CP3, CP5	IK6_U14

Kompetencje

Kod	Student jest gotów do:	Realizuje cel	Efekty kierunkowe
EU-K1	Student jest gotów do zapobiegania zagrożeniom dla bezpieczeństwa informacji.	CP1, CP2, CP3, CP5	IK6_K01, IK6_K03
EU-K2	Student jest gotów do zapewnienia kryptograficznej ochrony informacji przy wykorzystaniu współczesnych algorytmów kryptograficznych.	CP1, CP2, CP3, CP4, CP5	IK6_K01, IK6_K03

6. Treści programowe

Kod	Tematyka	wykład	ćwiczenia	Realizuje efekt
TP1	Wprowadzenie do przedmiotu. Zagrożenia dla bezpieczeństwa informacji i metody im zapobiegania. Podstawowe pojęcia i definicje z dziedziny kryptologii. Elementy teorii liczb: podzielność, kongruencje, arytmetyka modularna. Podstawowe zagadnienia algebry abstrakcyjnej: grupy, pierścienie, ciała.	2	2	EU-U1, EU-U2, EU-W1, EU-W2, EU-W3
TP2	Wprowadzenie do teorii szyfrów. Podział i rodzaje szyfrów klasycznych. Kodowanie alfabetu. Szyfry klasyczne: szyfr przesuwający, szyfr afiniczny, szyfr Vigenere'a, szyfr Hilla. Elementy kryptoanalizy ww. szyfrów.	2	2	EU-U1, EU-U3, EU-W1, EU-W2, EU-W3, EU-W4
TP3	Obliczanie odwrotności multiplikatywnej. Algorytm szybkiego potęgowania modularnego. Generator grupy multiplikatywnej. Algorytm Diffiego-Hellmana. Bezpieczeństwo algorytmu Diffiego-Hellmana.	2	4	EU-U1, EU-U2, EU-U4, EU-W5
TP4	Kryptosystem asymetryczny RSA. Algorytmy generacji kluczy, szyfrowania/deszyfrowania, generacji/weryfikacji podpisu cyfrowego RSA. Bezpieczeństwo kryptosystemu RSA.	2	4	EU-K1, EU-K2, EU-U1, EU-U4, EU-U5, EU-W3, EU-W5
TP5	Kryptosystem asymetryczny ElGamala. Algorytmy generacji kluczy, szyfrowania/deszyfrowania, generacji/weryfikacji podpisu cyfrowego ElGamala. Bezpieczeństwo kryptosystemu ElGamala.	2	4	EU-K1, EU-K2, EU-U1, EU-U4, EU-U5, EU-W3, EU-W5
TP6	Szyfry blokowe – idea szyfrowania blokowego. Konstrukcje współczesnych szyfrów blokowych. Specyfikacja szyfru blokowego AES. Tryby pracy szyfrów blokowych.	2	0	EU-K1, EU-K2, EU-U1, EU-U4, EU-U5, EU-W5

Kod	Tematyka	wykład	ćwiczenia	Realizuje efekt
TP7	Szyfry strumieniowe – idea szyfrowania strumieniowego. Konstrukcje szyfrów strumieniowych na bazie LFSR. Specyfikacja szyfru strumieniowego TRIVIUM.	2	0	EU-K1, EU-K2, EU-U1, EU-U4, EU-U5, EU-W5
TP8	Funkcje skrótu: idea skracania wiadomości, definicja funkcji skrótu, ataki ogólne na funkcje skrótu. Podstawowe konstrukcje funkcji skrótu: Merkle–Damgårda, Davisa Mayer'a, „sponge". Zastosowanie funkcji skrótu do kryptograficznej ochrony informacji. Funkcje skrótu SHA-3.	2	0	EU-K1, EU-K2, EU-U1, EU-U4, EU-U5, EU-W5

Razem godzin: 32

7. Metody kształcenia

Kod	Metoda
MK1	Wykład wsparty prezentacją komputerową.
MK2	Rozwiązywanie zadań pod nadzorem prowadzącego.
MK3	Samodzielnie rozwiązywanie zadań poza zajęciami.
MK4	Praca ze źródłami literaturowymi.

8. Nakład pracy studenta

Aktywność studenta	Obciążenie
Praca związana z przygotowaniem się do ćwiczeń.	15
Praca związana z przygotowaniem się do wykładu.	15
Przygotowanie do egzaminu	35
Przygotowanie do kolokwium	20
Praca z nauczycielem związana z: ćwiczenia	16
Praca z nauczycielem związana z: wykład	16
Liczba punktów ECTS (1 punkt=25h)	4
Procentowy udział pracy własnej studenta w sumarycznym obciążeniu studenta	72,65%
Sumaryczne obciążenie pracą studenta	117

9. Status zaliczenia przedmiotu

Egzamin pisemny

Forma studiów	Egzamin	Praca egzaminacyjna	Zaliczenie	Praca zaliczeniowa
niestacjonarne	×			

10. Metody weryfikacji efektów uczenia się

Składowe oceny końcowej

Forma sprawdzenia	Wybrana forma	Punktacja	Realizuje efekt
Egzamin pisemny	×	50	EU-K2, EU-U4, EU-U5, EU-U3, EU-W4, EU-W5, EU-K1, EU-U2, EU-U1, EU-W3, EU-W2, EU-W1
Egzamin ustny			
Sprawdzian pisemny			
Zaliczeniowy przegląd prac			
Referat pisemny			
Referat ustny			
Kolokwium	×	50	EU-K2, EU-U4, EU-U5, EU-U3, EU-W4, EU-W5, EU-K1, EU-U2, EU-U1, EU-W3, EU-W2, EU-W1
Praca domowa			
Miniprojekt			
Praca na zajęciach			
Projekt z dokumentacją			
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	TP1, TP2	MK1, MK2, MK3, MK4
EU-W2	CP1, CP2	TP1, TP2	MK1, MK2, MK3, MK4
EU-W3	CP1, CP2, CP3	TP1, TP2, TP4, TP5	MK1, MK2, MK3, MK4
EU-W4	CP2, CP3, CP4	TP2	MK1, MK2, MK3, MK4
EU-W5	CP2, CP3, CP5	TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4
EU-U1	CP1	TP1, TP2, TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4
EU-U2	CP1, CP2	TP1, TP3	MK1, MK2, MK3, MK4
EU-U3	CP2, CP3, CP4	TP2	MK1, MK2, MK3, MK4

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-U4	CP3, CP5	TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4
EU-U5	CP1, CP2, CP3, CP5	TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4
EU-K1	CP1, CP2, CP3, CP5	TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4
EU-K2	CP1, CP2, CP3, CP4, CP5	TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4

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	P6S_UW
EU-U2	IK6_U14	P6S_UW
EU-U3	IK6_U14	P6S_UW
EU-U4	IK6_U14	P6S_UW
EU-U5	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, Wydawnictwa Naukowo Techniczne, 2005
2. Janusz Szmidt, Michał Misztal, Wstęp do kryptologii, WSISIZ, 2004
3. Marcin Karbowski, Podstawy kryptografii, Helion, 2014

Literatura uzupełniająca

1. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii., Helion, 2012

14. Informacje o nauczycielach akademickich

Osoby odpowiedzialne za przedmiot

1. dr inż. Piotr Mroczkowski

Osoby prowądzace przedmiot

1. dr inż. Piotr Mroczkowski