KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE

PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA IM. WITELONA W LEGNICY
WYDZIAŁ NAUK TECHNICZNYCH I EKONOMICZNYCH

Kierunek studiów:		**INFORMATYKA**				
Poziom studiów:		studia pierwszego stopnia				
Profil studiów:		praktyczny				
Forma studiów:		stacjonarne/niestacjonarne				
Nazwa modułu:		**Kryptografia i bezpieczeństwo danych**				
Rodzaj modułu:		specjalnościowy				
Język wykładowy:		Język polski*				
Rok studiów:	II	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**				
Semestr:	IV	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba punktów ECTS ogółem:	2	30/12	-	15/12	-	-
Forma zaliczenia:		Zaliczenie na ocenę.				
Wymagania wstępne:		Podstawowa wiedza z zakresu matematyki, szczególnie dyskretnej oraz metod probabilistycznych i statystyki.				

II. CELE KSZTAŁCENIA

Cele kształcenia:

Cel 1: Zaznajomienie studentów z podstawowymi zadaniami kryptografii.
Cel 2: Zapoznanie słuchaczy z algorytmami szyfrowania.
Cel 3: Zapoznanie słuchaczy z metodami zapewnienia bezpieczeństwa.

III. EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW

Efekt	Student, który zaliczył moduł w zakresie:	Odniesienie do efektów kierunkowych	Metody weryfikacji
	wiedzy:		
W01	Student ma podstawą wiedzę na temat metod szyfrowania, zna podstawowe techniki kryptograficzne oraz podstawowe trendy rozwojowe w kryptografii i bezpieczeństwie danych.	K1I_W01, K1I_W06, K1I_W09, K1I_W12	Kolokwium pisemne z wykładu.
	umiejętności:		
U01	Potrafi zastosować zdobytą wiedzę m.in. do zarządzania kluczami szyfrowania.	K1I_U06, K1I_U13	Kolokwium na laboratorium.
	kompetencji społecznych:		
K01	Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje.	K1I_K01	Obserwacja zachowań studentów.

IV. TREŚCI PROGRAMOWE

Treści programowe (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)

Wykład

Kod	Tematyka zajęć	Liczba godzin S/N
w01	Kryptografia - szyfrowanie i historia.	2/1
w02	Podstawowe techniki szyfrowania.	2/1
w03	Algorytmy symetryczne.	4/1

w04	Algorytmy asymetryczne –RSA.	4/1
w05	Funkcje haszujące.	4/1
w06	Liczby pseudolosowe.	2/1
w07	Podpisy cyfrowe.	4/1
w08	Uwierzytelnianie.	2/1
w09	Administracja kluczami.	4/2
w10	Kolokwium pisemne z wykładu.	2/2

Laboratorium

Kod	Tematyka zajęć	Liczba godzin S/N
lab01	Kryptografia - szyfrowanie i historia.	1/1
lab02	Podstawowe techniki szyfrowania.	1/1
lab03	Algorytmy symetryczne.	2/1
lab04	Algorytmy asymetryczne –RSA.	2/1
lab05	Funkcje haszujące.	1/1
lab06	Liczby pseudolosowe.	1/1
lab07	Podpisy cyfrowe.	1/1
lab08	Uwierzytelnianie.	2/1
lab09	Administracja kluczami.	2/2
lab10	Kolokwium.	2/2

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia:

Wykład multimedialny.
Ćwiczenia problemowe przy komputerze.

2. Narzędzia (środki) dydaktyczne:

Tablica multimedialna, komputer.

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

Forma zaliczenia modułu.
Zaliczenie na ocenę.

Kryteria oceny formującej*:**
1. Krótkie zadania domowe.
2. Umiejętność samodzielnego rozwiązywania zadań przy komputerze.

Kryteria oceny podsumowującej***
1. Kolokwium pisemne z wykładu:
50-59% - ocena dostateczna,
60-69% - ocena dostateczna plus,
70-79% - ocena dobra,
80-89% - ocena dobra plus,
powyżej 90% - ocena bardzo dobra.

2. Kolokwium na laboratorium:
50-59% - ocena dostateczna,
60-69% - ocena dostateczna plus,
70-79% - ocena dobra,
80-89% - ocena dobra plus,
powyżej 90% - ocena bardzo dobra.

Na ocenę 3,0: student zna podstawowe metody i narzędzia, potrafi przy pomocy prowadzącego rozwiązać proste zadania.
Na ocenę 3,5: zna podstawowe metody i narzędzia, potrafi samodzielnie rozwiązać proste zadania.
Na ocenę 4,0: zna metody i narzędzia omawiane na zajęciach, potrafi je samodzielnie zastosować. Z pomocą

prowadzącego potrafi rozwiązać zadania typowe.
Na ocenę 4,5: zna metody i narzędzia omawiane na zajęciach, potrafi je samodzielnie zastosować. Samodzielnie potrafi rozwiązać zadania typowe.
Na ocenę 5,0: zna metody i narzędzia omawiane na zajęciach, potrafi je samodzielnie zastosować. Samodzielnie potrafi rozwiązać zadania typowe. Jest aktywny na zajęciach.

Ocena podsumowująca*:**
Ocena z modułu: średnia ocen z poszczególnych form zajęć.

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	45/24
Udział w wykładach	30/12
Udział w innych formach zajęć (laboratorium)	15/12
Inne (udział w egzaminie)	-
Samodzielna praca studenta (godziny niekontaktowe)	5/26
Przygotowanie do wykładu	0/10
Przygotowanie do innych form zajęć (laboratorium)	0/11
Przygotowanie do egzaminu	-
Przygotowanie do zaliczenia innych zajęć (laboratorium)	5
Inne (np. gromadzenie materiałów do projektu, kwerenda internetowa, opracowanie prezentacji multimedialnej itp.)	-
Łączna liczba godzin	50
Punkty ECTS za moduł	2

VIII. ZALECANA LITERATURA

Literatura podstawowa:
1. M. Kutyłowski, W-B. Strothmann. *Kryptografia*. ReadMe 1999.
2. M. Karbowski. *Podstawy kryptografii*. Helion 2014.

Literatura uzupełniająca:
1. D. R. Stinson. *Kryptografia*. WNT 2005.

*należy odpowiednio wypełnić

**należy wpisać formę/formy przypisane do modułu określone w programie studiów (wykład, ćwiczenia, seminarium, konwersatorium, lektorat, laboratorium, warsztat, projekt, zajęcia praktyczne, zajęcia terenowe, zajęcia wychowania fizycznego, praktyka zawodowa, inne)

*** proszę wpisać odpowiednie kryteria oceny formującej i podsumowującej