I. KARTA PRZEDMIOTU

1. Nazwa przedmiotu: **BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH**
2. Kod przedmiotu: **Bsi**
3. Jednostka prowadząca: **Wydział Mechaniczno-Elektryczny**
4. Kierunek: **Mechatronika**
5. Specjalność: **Zastosowanie informatyki w mechatronice**
6. Moduł: **Moduł informatyki i elektroniki**
7. Poziom studiów: **II stopnia**
8. Forma studiów: **niestacjonarne**
9. Semestr studiów: **III**
10. Profil: **ogólnoakademicki**
11. Prowadzący: **dr Przemysław Rodwald**

CEL PRZEDMIOTU

C1	Zapoznanie studentów z zagadnieniami bezpieczeństwa informatycznego, kryptografią symetryczną i asymetryczną oraz algorytmami integralności danych.

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1	Znajomość algebry Boola.
2	Podstawowa obsługa komputera.

EFEKTY KSZTAŁCENIA

EK1	ma podstawową wiedzę zakresu bezpieczeństwa systemów informatycznych i kryptografii
EK2	potrafi wykorzystać techniki kryptograficzne w praktyce

TREŚCI PROGRAMOWE

	WYKŁADY	Liczba godzin
W1	Wprowadzenie do zagadnień bezpieczeństwa informatycznego.	**1**
W2	Klasyczne techniki szyfrowania i steganografia.	**1**
W3	Kryptografia symetryczna (szyfry i funkcje skrótu).	**2**
W4	Kryptografia asymetryczna i podpisy cyfrowe.	**2**
W5	Podpisy cyfrowe.	**2**
	Razem	**8**
	ĆWICZENIA	
Ć1	Systemy liczbowe (dwójkowy, heksadecymalny).	**2**
	Razem	**2**
	ZAJĘCIA LABORATORYJNE	
L1	Szyfry historyczne.	**1**
L2	Steganografia.	**1**
L3	Funkcje skrótu.	**2**
L4	Bezpieczny email.	**2**
L5	Podpisy cyfrowe.	**2**
	Razem	**8**

NARZĘDZIA DYDAKTYCZNE

1	Notebook z projektorem
2	Tablica i kolorowe pisaki

3	Laboratorium komputerowe

SPOSOBY OCENY

PODSUMOWUJĄCA

P1	Kolokwium	EK1
P2	Wykonanie sprawozdania z zajęć laboratoryjnych	EK2

OBCIĄŻENIE PRACĄ STUDENTA

Forma aktywności	**Średnia liczba godzin na zrealizowanie aktywności**	
semestr	**III**	**razem**
udział w wykładach	8	8
udział w ćwiczeniach	2	2
udział w zajęciach laboratoryjnych	8	8
Samodzielne opracowanie zagadnień	10	10
Konsultacje	2	2
SUMA GODZIN W SEMESTRZE	**30**	**30**
PUNKTY ECTS W SEMESTRZE	**1**	**1**

LITERATURA

PODSTAWOWA

1	William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Matematyka szyfrów i techniki kryptologii, Wydawnictwo Helion, 2011
2	William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Koncepcje i metody bezpiecznej komunikacji, Wydawnictwo Helion, 2012

UZUPEŁNIAJĄCA

3	Menezes A.J. , P. van Oorschot, Vanstone S.A., Kryptografia stosowana, WNT, 2005

PROWADZĄCY PRZEDMIOT

1	dr Przemysław Rodwald, p.rodwald@amw.gdynia.pl

Formy oceny

Efekt	Na ocenę 2	Na ocenę 3	Na ocenę 4	Na ocenę 5
EK1	*ma podstawową wiedzę zakresu bezpieczeństwa systemów informatycznych i kryptografii*			
	student uzyskał poniżej 50% możliwych do zdobycia punktów	student uzyskał co najmniej 50% i nie więcej niż 60% możliwych do zdobycia punktów (3.0) student uzyskał co najmniej 60% i nie więcej niż 70% możliwych do zdobycia punktów (3.5)	student uzyskał co najmniej 70% i nie więcej niż 80% możliwych do zdobycia punktów (4.0) student uzyskał co najmniej 80% i nie więcej niż 90% możliwych do zdobycia punktów (4.5)	student uzyskał co najmniej 90% możliwych do zdobycia punktów (5.0)
EK2	*potrafi wykorzystać techniki kryptograficzne w praktyce*			
	student uzyskał poniżej 50% możliwych do zdobycia punktów	student uzyskał co najmniej 50% i nie więcej niż 60% możliwych do zdobycia punktów (3.0)student uzyskał co najmniej 60% i nie więcej niż 70% możliwych do zdobycia punktów (3.5)	student uzyskał co najmniej 70% i nie więcej niż 80% możliwych do zdobycia punktów (4.0)student uzyskał co najmniej 80% i nie więcej niż 90% możliwych do zdobycia punktów (4.5)	student uzyskał co najmniej 90% możliwych do zdobycia punktów (5.0)