



### KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	<b>M#1-S1-IB-KiK-612</b>
	studia niestacjonarne:	
Nazwa przedmiotu	<b>Nowoczesne Metody Kryptograficzne</b>	
Nazwa przedmiotu w języku angielskim	<b>Modern Cryptographic Methods</b>	
Obowiązuje od roku akademickiego	<b>2022/2023</b>	

### USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	<b>INŻYNIERIA BEZPIECZEŃSTWA</b>
Poziom kształcenia	<b>I stopień</b>
Profil studiów	<b>ogólnoakademicki</b>
Forma i tryb prowadzenia studiów	<b>Studia stacjonarne</b>
Zakres	<b>Kryminologia i Kryminalistyka</b>
Jednostka prowadząca przedmiot	<b>Katedra Technik Komputerowych i Uzbrojenia</b>
Koordinator przedmiotu	<b>dr inż. Piotr Thomas</b>
Zatwierdził	

### OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	<b>Przedmiot specjalnościowy</b>	
Status przedmiotu	<b>Obowiązkowy</b>	
Język prowadzenia zajęć	<b>Polski</b>	
Usytuowanie w planie studiów - semestr	studia stacjonarne	<b>Semestr VI</b>
	studia niestacjonarne	
Wymagania wstępne	<b>brak</b>	
Egzamin (TAK/NIE)	<b>NIE</b>	
Liczba punktów ECTS	<b>2</b>	

Forma prowadzenia zajęć		wykład	ćwiczenia	laboratorium	projekt	inne
Liczba godzin w semestrze	studia stacjonarne:	15		15		
	studia niestacjonarne:					

### EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Ma podstawową wiedzę na temat współczesnych metod zapewnienia bezpieczeństwa przesyłania informacji. Posiada podstawową wiedzę na temat zagrożeń z tym związanych.	IB1_W21
	W02	Dysponuje podstawową wiedzą na szyfrowania i deszyfrowania danych i podstawowych algorytmów.	IB1_W21
Umiejętności	U01	Potrafi zastosować podstawowe algorytmy służące szyfrowaniu i deszyfrowaniu danych.	IB1_U34
Kompetencje społeczne	K01	Rozumie potrzebę dokształcania się i podnoszenia swoich kompetencji zawodowych w zakresie monitorowania zagrożeń.	IB1_K01
	K02	Potrafi pracować w zespole.	IB1_K04

### TREŚCI PROGRAMOWE

Forma zajęć*	Treści programowe
wykład	Kryptografia klasyczna – podstawowa terminologia. Klasyfikacja zagrożeń. Proste szyfry. Algorytmy kryptograficzne. Współczesne kryptogramy. Poufność i uwierzytelnianie.
laboratorium	Zastosowanie algorytmów służących do szyfrowania i deszyfrowania informacji. Zastosowanie mechanizmów kryptograficznych.

### METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia (zaznaczyć X)					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
W02			X			
U01					X	
K01						X
K02						X

## FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia	Warunki zaliczenia
wykład	<b>Zaliczenie z oceną</b>	Uzyskanie co najmniej połowy punktów z kolokwium zaliczeniowego.
laboratorium	<b>Zaliczenie z oceną</b>	Złożenie wszystkich sprawozdań z ćwiczeń laboratoryjnych. Obecność na zajęciach..

## NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
		W	C	L	P	S	W	C	L	P	S	
1.	Udział w zajęciach zgodnie z planem studiów	15		15								h
2.	Inne (konsultacje, egzamin)	2		2								h
3.	<b>Razem przy bezpośrednim udziale nauczyciela akademickiego</b>	<b>34</b>										h
4.	<b>Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego</b>	<b>1,4</b>										ECTS
5.	<b>Liczba godzin samodzielnej pracy studenta</b>	<b>16</b>										h
6.	<b>Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy</b>	<b>0,6</b>										ECTS
7.	<b>Nakład pracy związany z zajęciami o charakterze praktycznym</b>	<b>25</b>										h
8.	<b>Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym</b>	<b>1,0</b>										ECTS
9.	<b>Sumaryczne obciążenie pracą studenta</b>	<b>50</b>										h
10.	<b>Punkty ECTS za moduł</b> <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	<b>2</b>										ECTS

## LITERATURA

1. M. Kutyłowski i W. B. Strothmann Kryptografia: Teoria i praktyka zabezpieczania systemów komputerowych, Wyd. READ ME, Warszawa, 1999,
2. B. Schneier: Kryptografia dla praktyków, WNT, Warszawa, 2002, wydanie drugie
3. D. R. Stinson, Kryptografia, WNT, Warszawa, 2005
4. R. Wobst, Kryptologia. Budowa i łamanie zabezpieczeń, RM, Warszawa, 2002