

KARTA PRZEDMIOTU

<i>Nazwa przedmiotu w języku polskim:</i> ELEMENTY KRYPTOGRAFII I SZYFROWANIA								<i>Kod przedmiotu:</i> KNS/BW-IIP/BC/60	
<i>Nazwa przedmiotu w języku angielskim:</i> ENCRYPTION AND CRYPTOGRAPHY ELEMENTS									
<i>Kierunek studiów:</i> Bezpieczeństwo wewnętrzne			<i>Profil:</i> praktyczny			<i>Poziom studiów:</i> II stopień			
<i>Specjalność/specjalizacja:</i> Bezpieczeństwo cyberprzestrzeni			<i>Forma zaliczenia przedmiotu:</i> zaliczenie na ocenę			<i>Semestr studiów:</i> 4			
<i>Nazwa grupy zajęć:</i> zajęcia specjalnościowe			<i>Język w jakim prowadzone są zajęcia:</i> polski						
<i>Tryb studiów</i>	<i>Forma zajęć</i>							<i>Ogólna liczba godzin</i>	<i>Liczba punktów ECTS:</i>
	<i>W</i>	<i>Ćw.</i>	<i>Konw.</i>	<i>Lab.</i>	<i>Proj.</i>	<i>Sem.</i>	<i>Zajęcia terenowe</i>		
<i>Tryb stacjonarny</i>			-	30	-	-	-	30	3
<i>Tryb niestacjonarny</i>			-	30	-	-	-	30	
<i>Jednostka realizująca przedmiot, wydział:</i> Kolegium Nauk Społecznych									
<i>Odpowiedzialny za opracowanie karty przedmiotu (tytuł/stopień naukowy, imię i nazwisko, adres e-mail):</i> dr Marcin Sobota, msobota@wszop.edu.pl									
CEL PRZEDMIOTU									
C1.	Przekazanie wiedzy na temat podstaw teoretycznych w kryptografii.								
C2.	Przekazanie wiedzy na temat potrzeby zabezpieczania danych, nośników danych, łączności i transmisji danych i doboru środków do specyfikacji danych i środków wymiany danych.								
WYMAGANIA WSTĘPNE									
1.	Wiedza z przedmiotów: Technologia informacyjna i Sieci komputerowe								
2.	Umiejętności matematyczne w zakresie szkoły średniej								

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ		METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ	ODNIESIENIE DO:		
			TREŚCI PROGRAMOWYCH	KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ	
EU1	Student zna metody szyfrowania danych.	sprawozdania z laboratorium	L1-L10	BWII K_W 08	
EU2	Student jest świadomy potrzeby zabezpieczania danych i dobiera właściwe metody do specyfiki danych i środków wymiany danych.	sprawozdania z laboratorium	L1-L10	BWII K_U 06	
EU3	Student wykorzystuje specjalistyczne oprogramowanie służące do szyfrowania.	sprawozdania z laboratorium	L1-L10	BWII K_U 02	
L.p.	LABORATORIUM			Liczba godzin	
				S	N
L1	Praca z prostymi kryptosystemami.			3	3
L2	Przygotowanie środowiska do testów.			3	3
L3	Kontrola dostępu do danych i silne szyfrowanie nośników danych.			3	3
L4	Stosowanie szyfrowania do anonimizacji danych.			3	3
L5	Stosowanie funkcji skrótu.			3	3
L6	Standardy szyfrowania dla sieci bezprzewodowych.			3	3
L7	Techniki tunelowania.			3	3
L8	Funkcje skrótu.			3	3
L9	Kryptoanaliza.			3	3
L10	Steganografia i metody alternatywne.			3	3
RAZEM				30	30
FORMA I KRYTERIA ZALICZENIA WYKŁADU: egzamin pisemny (pytania otwarte) - ocena jakościowa,					
METODY I FORMY DYDAKTYCZNE					
1.	objaśnienie				
2.	ćwiczenia laboratoryjne				
3.	praca indywidualna				
4.	praca grupowa				
NARZĘDZIA DYDAKTYCZNE					
1.	laboratorium komputerowe				
2.	platforma e-learningowa				
OPROGRAMOWANIE					
1.	MS Powerpoint				
2.	Microsoft Office Professional Edition 2010				

3.	VeraCrypt
4.	BoxCryptor

OBCIĄŻENIE STUDENTA PRACĄ

Forma aktywności		Liczba godzin na zrealizowanie aktywności	
		tryb stacjonarny	tryb niestacjonarny
1.	godziny kontaktowe z nauczycielem akademickim	30	30
2.	samodzielne przygotowanie się do zajęć	15	15
3.	przygotowanie do zaliczenia/egzaminu	15	15
4.	konsultacje	2	2
5.	zapoznanie się z literaturą	13	13
6.	zaliczenie/egzamin	-	-
SUMA GODZIN		75	75
LICZBA PUNKTÓW ECTS		3	3

LITERATURA PODSTAWOWA

1.	J.P. Aumasson: Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, Wyd. PWN, 2018
2.	M. Karbowski: Podstawy kryptografii, wyd. Helion, 2014
3.	B. Schneier: Kryptografia dla praktyków, wyd. WNT, 2002

LITERATURA UZUPEŁNIAJĄCA I ŹRÓDŁA PRAWA

1.	D. E. Robling-Denning: Kryptografia i ochrona danych, WNT, 1992
2.	W. Stallings: Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii, wyd. Helion, 2011
3.	M. Sawerwain, J. Wiśniewska: Informatyka kwantowa. Wybrane obwody i algorytmy, wyd. Helion, 2015
4.	C. McNab: Ocena bezpieczeństwa sieci, wyd. APN Promise, 2017

INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE:

1.	<p>PLATFORMA MOODLE zawiera:</p> <ul style="list-style-type: none"> ▪ materiały dydaktyczne do przedmiotu ▪ przedmiotowe efekty uczenia się ▪ zalecaną literaturę ▪ warunki i kryteria zaliczenia przedmiotu
2.	BIBLIOTEKA WSZOP zapewnia literaturę podstawową do przedmiotu oraz wybrane pozycje literatury uzupełniającej, w tym dostęp do zbiorów cyfrowych i Platformy IBUK Libra
3.	<p>ELEKTRONICZNY NIEZBĘDNIK STUDENTA zawiera:</p> <ul style="list-style-type: none"> ▪ kierunkowe efekty uczenia się ▪ karty przedmiotów ▪ terminy konsultacji nauczycieli akademickich
4.	<p>WIRTUALNY DZIEKANAT zawiera:</p> <ul style="list-style-type: none"> ▪ harmonogram zajęć na bieżący semestr ▪ harmonogram sesji egzaminacyjnej ▪ ogłoszenia dotyczące organizacji roku akademickiego
5.	<p>Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny jakościowej oznacza, że zakładane efekty zostały osiągnięte:</p> <ul style="list-style-type: none"> ▪ w pełni – ocena bardzo dobry ▪ z niewielkimi niedociągnięciami – ocena dobry plus ▪ z brakami, które można uzupełnić – ocena dobry ▪ z istotnymi brakami, które można uzupełnić – ocena dostateczny plus ▪ z istotnymi brakami na minimalnym poziomie – ocena dostateczny lub ▪ nie zostały osiągnięte – ocena niedostateczny.

6.	Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny ilościowej oznacza, że zakładane efekty zostały osiągnięte: <ul style="list-style-type: none">▪ 91-100% sumy – ocena bardzo dobry▪ 81-90% – ocena dobry plus▪ 71-80% – ocena dobry▪ 61-70% – ocena dostateczny plus▪ 51-60% – ocena dostateczny lub▪ 50% i mniej – ocena niedostateczny.
7.	Terminy egzaminów uzgadnia starosta roku z prowadzącym zajęcia
8.	Karta przedmiotu obowiązuje od roku akademickiego 2024/25