

# AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

## KARTA OPISU PRZEDMIOTU

<b>Wydział</b>		<b>Informatyki</b>	
<b>Kierunek</b>		<b>Informatyka</b>	
<b>Specjalność</b>			
<b>Semestr</b>	<b>II</b>	<b>Program studiów, dla którego obowiązuje sylabus</b>	<b>2024/2025</b>
<b>Stopień studiów</b>	<b>II</b>		

Nazwa przedmiotu	Kryptografia			
Kod przedmiotu	KRYPT			
Łączna liczba godzin	30	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	wykład			
Język przedmiotu	polski			
Liczba punktów ECTS	3			

<b>Prowadzący zajęcia</b>	
<b>Forma prowadzonych zajęć</b>	<b>Wykład</b>
<b>Wymiar zajęć</b>	<b>30 h</b>
<b>Stopień (tytuł) naukowy</b>	
<b>Imię</b>	
<b>Nazwisko</b>	

<b>Wymagania wstępne</b>	Znajomość podstaw matematyki dyskretniej, metod probabilistycznych, statystyki, programowania, algorytmów i struktur danych.
<b>Założenia i cele przedmiotu</b>	Przedmiot ma na celu zapoznanie studentów z podstawowymi zasadami, metodami i zastosowaniami kryptografii w ochronie informacji. Studenci poznają kluczowe pojęcia oraz różnorodne techniki szyfrowania i deszyfrowania danych oraz są wprowadzani w zagadnienia związane z podpisami cyfrowymi, steganografią oraz podstawami kryptoanalizy, przygotowujące ich do praktycznego zastosowania tych technik w celu zabezpieczania danych i komunikacji. Kurs umożliwi zrozumienie, jak kryptografia zapewnia poufność, integralność i autentyczność informacji w systemach teleinformatycznych.
<b>Metody dydaktyczne</b>	1. Wykład – w formie tradycyjnej lub prezentacji multimedialnej – z elementami dyskusji

<b>Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji)</b>		<b>Odniesienie do efektów dla kierunku</b>	<b>Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji</b>
WIEDZA – absolwent zna i	W01.Sposoby ochrony własności przed niepowołanym dostępem.	K_W01 K_W07	P7S_WG P7S_WG_INŻ

## AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

rozumie:	W02. Normy z zakresu bezpieczeństwa komputerowego.	K_W09	
UMIEJĘTNOŚCI – absolwent potrafi:	U01. Zastosować praktyczne metody realizacji algorytmów kryptograficznych do ochrony baz danych, plików dyskowych i poczty elektronicznej. U02. Ocenąć przydatność programów oferowanych przez dostawców oprogramowania związanego z kryptografią i podpisem cyfrowym.	K_U01 K_U03 K_U06 K_U17	P7S_UW P7S_UW INŻ P7S_KK P7S_UK
KOMPETENCJE SPOŁECZNE – absolwent jest gotów do	K01. Ciągłego samokształcenia się.	K_K03	P7S_UU

Treści programowe		
Lp.	Tematyka zajęć	Liczba godzin
<b>Forma zajęć – wykład</b>		
1	Podstawowe pojęcia: szyfr podstawieniowy, przestawieniowy, blokowy, strumieniowy, symetryczny (z kluczem tajnym), asymetryczny (z kluczem publicznym), szyfry historyczne.	4
2	Szyfry symetryczne: przykłady symetrycznych szyfrów blokowych i strumieniowych.	4
3	Szyfry asymetryczne: szyfr RSA, szyfr ElGamala	4
4	Infrastruktura klucza publicznego (PKI), podpisy cyfrowe.	4
5	Szyfrowanie hybrydowe: RSA – AES.	2
6	Programy do ochrony informacji.	4
7	Ochrona plików dyskowych i poczty elektronicznej przed niepożądanym dostępem, protokół secure e-mail.	4
8	Steganografia i kryptosteganografia.	2
9	Elementy kryptoanalizy.	2

<b>Forma i warunki zaliczenia przedmiotu</b>	Kolokwium z wykładu.	
<b>Metody weryfikacji efektów uczenia się</b>		<b>Nr efektu uczenia się z sylabusu</b>
	Kolokwium pisemne	W01-W02, U01-U02, K01

<b>Literatura podstawowa</b>	<ol style="list-style-type: none"> <li>1. M. Karbowski, <i>Podstawy kryptografii</i>, Helion, Gliwice 2014.</li> <li>2. C. Kościelny, M. Kurkowski, M. Srebrny, <i>Kryptografia. Teoretyczne podstawy i praktyczne zastosowania</i>, Wydawnictwo PJWSTK, Warszawa 2009.</li> </ol>
<b>Literatura uzupełniająca</b>	<ol style="list-style-type: none"> <li>1. D. Stinson, <i>Kryptografia. W teorii i w praktyce</i>,</li> </ol>

## AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

	WNT, Warszawa 1995. 2. N. Ferguson, B. Schneier, <i>Kryptografia w praktyce</i> , Helion, Gliwice 2004.
--	--

Nakład pracy studenta	
	Liczba godzin
Zajęcia dydaktyczne	30
Przygotowanie się do zajęć	15
Studiowanie literatury	13
Udział w konsultacjach	2
Przygotowanie projektu / eseju / prezentacji itp.	0
Przygotowanie się do egzaminu / zaliczenia	20
Inne	-
<b>ŁĄCZNY nakład pracy studenta w godz.</b>	<b>80</b>
<b>Liczba punktów ECTS</b>	<b>3</b>