Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-I2C-2000-s1
	studia niestacjonarne:	E-1IZ2C-1001-s1
Nazwa przedmiotu	**Matematyczne podstawy kryptologii**	
Nazwa przedmiotu w języku angielskim	**Mathematical foundations of cryptology**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**II stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia stacjonarne i niestacjonarne**
Zakres	**Cyberbezpieczeństwo**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**Dr inż. Justyna Kęczkowska**
Zatwierdził	**Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki dr hab. inż. Roman Deniziak, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		**Przedmiot specjalnościowy**
Status przedmiotu		**Obowiązkowy**
Język prowadzenia zajęć		**Polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**Semestr I**
	studia niestacjonarne	**Semestr I**
Wymagania wstępne		Podstawowa wiedza z algebry liniowej, teorii grup, teorii liczb oraz rachunku prawdopodobieństwa.
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**4**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**	**30**			
	studia niestacjonarne:	**18**	**18**			

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie matematyczne podstawy tworzenia systemów kryptograficznych.	INF2_W01, INF2_W04, INF2_W07
Umiejętności	U01	Student potrafi wyjaśnić matematyczne podstawy poznanych kryptosystemów wraz z dowodami ich poprawności.	INF2_U01, INF2_U05, INF2_U06
Kompetencje społeczne	K01	Student jest przygotowany do uzupełniania swojej wiedzy, umie ocenić stopień zrozumienia przez siebie problemu.	INF2_K03

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Wstęp do rodzajów systemów kryptograficznych** (modele szyfrowania symetrycznego/ asymetrycznego). 2. **Podstawy teorii liczb i ciał skończonych** (podzielność, rozkład na czynniki, liczby pierwsze, reprezentacje liczb całkowitych w różnych bazach, NWD, NWW, kongruencje, grupy, pierścienie i ciała, arytmetyka dużych liczb całkowitych, arytmetyka wielomianowa, ciała skończone postaci GF(p)). 3. **Matematyczne podstawy klasycznych techniki szyfrowania** (modele matematyczne kodowania/dekodowania wiadomości). 4. **Matematyczna (statystyczna) teoria informacji Shannona** (modele źródeł, miary ilości informacji, podstawowe twierdzenia o kodowaniu). 5. **Matematyczne podstawy zaawansowanych standardów szyfrowania** (arytmetyka ciał skończonych, funkcje transformacyjne AES, wielomiany o współczynnikach z GF(28)). 6. **Zaawansowana teoria liczb** (twierdzenie Fermata i Eulera, logarytmy dyskretne, chińskie twierdzenie o resztach, generowanie liczb pierwszych, testy pierwszości, liczby losowe). 7. **Matematyczne podstawy systemów kryptografii z kluczami publicznymi** (algorytm RSA, system kryptograficzny ElGamal, arytmetyka krzywych eliptycznych, generatory liczb pseudolosowych). 8. **Teoria funkcji skrótu** (wymagania stawiane funkcjom haszującym, matematyczne podstawy paradoksu urodzin, algorytmy SHA). 9. **Teoria podpisów cyfrowych** (mechanizmy generowania podpisu cyfrowego, problem faktoryzacji, problem logarytmu dyskretnego, faktoryzacji krzywych eliptycznych). 10. **Przesyłanie informacji tajnych** (funkcje wykorzystywane do uwierzytelniania komunikatów).

ćwiczenia	1. **Podstawy teorii liczb i ciał skończonych** (podzielność, rozkład na czynniki, liczby pierwsze, reprezentacje liczb całkowitych w różnych bazach, NWD, NWW, kongruencje, grupy, pierścienie i ciała, arytmetyka dużych liczb całkowitych, arytmetyka wielomianowa, ciała skończone postaci GF(p)). 2. **Matematyczne podstawy klasycznych techniki szyfrowania** (modele ma-tematyczne kodowania/dekodowania wiadomości). 3. **Matematyczna (statystyczna) teoria informacji Shannona** (modele źródeł, miary ilości informacji, podstawowe twierdzenia o kodowaniu). 4. **Matematyczne podstawy zaawansowanych standardów szyfrowania** (arytmetyka ciał skończonych, funkcje transformacyjne AES, wielomiany o współczynnikach z GF(28)). 5. **Zaawansowana teoria liczb** (twierdzenie Fermata i Eulera, logarytmy dyskretne, chińskie twierdzenie o resztach, generowanie liczb pierwszych, testy pierwszości, liczby losowe). 6. **Matematyczne podstawy systemów kryptografii z kluczami publicznymi** (algorytm RSA, system kryptograficzny ElGamal, arytmetyka krzywych eliptycznych, generatory liczb pseudolosowych). 7. **Teoria funkcji skrótu** (wymagania stawiane funkcjom haszującym, matematyczne podstawy paradoksu urodzin, algorytmy SHA). 8. **Teoria podpisów cyfrowych** (mechanizmy generowania podpisu cyfrowe-go, problem faktoryzacji, problem logarytmu dyskretnego, faktoryzacji krzywych eliptycznych).

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
U01			X			
K01			X			

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium
ćwiczenia	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30	**30**				**18**	**18**				
2.	Inne (konsultacje, egzamin)	**2**	**2**				**2**	**2**				h

3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**64**	**40**	h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2.56**	**1.6**	ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**36**	**60**	h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**1.44**	**2.4**	ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**30**	**18**	h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1.20**	**0.72**	ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**100**	**100**	h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**4**		ECTS

LITERATURA

1. D. R. Stinson, M. Paterson, Kryptografia W teorii i praktyce, Wydawnictwo Naukowe PWN, Warszawa 2021 (wyd. 4).
2. M. Karbowski, Podstawy kryptografii, Wydawnictwo HELION, Gliwice 2014.
3. I. Blake, G. Seroussi, N. Smart, Krzywe eliptyczne w kryptografii, WNT, Warszawa 2014.
4. D. Stinson, Kryptografia w teorii i praktyce, WNT, Warszawa 2005.
5. T. Adamski, Zbiór zadań z podstaw teoretycznych kryptografii i ochrony informacji, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2014.