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

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-01-s2
	studia niestacjonarne:	E-1IZ2C-1001-s2
Nazwa przedmiotu	**Kryptografia i kryptoanaliza**	
Nazwa przedmiotu w języku angielskim	**Cryptography and Cryptoanalysis**	
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 Urządzeń Elektrycznych i Automatyki**
Koordynator przedmiotu	**Dr inż. Michał Łaskawski**
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 II**
	studia niestacjonarne	**Semestr II**
Wymagania wstępne		**Wprowadzenie do cyberbezpieczeństwa, Matematyczne podstawy kryptologii**
Egzamin (TAK/NIE)		**TAK**
Liczba punktów ECTS		**5**

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	Zna i rozumie zagrożenia dotyczące systemów informatycznych oraz narzędzia z zakresu kryptografii i kryptoanalizy pozwalające je wykrywać, usuwać lub im przeciwdziałać.	INF2_W06
	W02	Zna i rozumie zasady oraz algorytmy kryptosystemów pozwalające tworzyć oprogramowanie spełniające wymogi bezpieczeństwa.	INF2_W01, INF2_W04, INF2_W06, INF2_W07
Umiejętności	U01	Potrafi, przy użyciu odpowiednich metod i narzędzi z zakresu kryptoanalizy, przeprowadzić czynności audytowe pozwalające ocenić stan zabezpieczenia systemu informatycznego i wskazać ewentualne braki.	INF2_U01, INF2_U05, INF2_U06, INF2_U07
	U02	Potrafi, przy użyciu kryptosystemów, zapobiegać zagrożeniom i zabezpieczać systemy informatyczne.	INF2_U06, INF2_U07, INF2_U09
Kompetencje społeczne	K01	Rozumie potrzebę ciągłego podnoszenia kompetencji i uświadamiania użytkowników narzędzi informatycznych w zakresie cyberbezpieczeństwa.	INF2_K03, INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
Wykład	1. **Kryptografia klasyczna, wybrane proste kryptosystemy i ich implementacje** (szyfry: przestawieniowy, podstawieniowy, afiniczny, Vigenere'a, Hilla, permutacyjny, strumieniowy). 2. **Kryptoanaliza wybranych algorytmów kryptograficznych** (analiza szyfru afinicznego, podstawieniowego, Vigenere'a, Hilla, permutacyjnego i strumieniowego). 3. **Pojęcie doskonałej poufności** (teoria prawdopodobieństwa, tajność doskonała, entropia). 4. **Szyfry strumieniowe i blokowe** (sieci podstawieniowy-permutacyjne, kryptoanaliza liniowa i różnicowa, implementacje i zastosowanie DES, AES). 5. **Standardy i implementacje funkcji mieszających** (integralność danych i bezpieczeństwo funkcji mieszającej, iterowane funkcje mieszające, SHA-3). 6. **Uwierzytelnianie wiadomości** (kody uwierzytelniania wiadomości, bezwarunkowo bezpieczne kody). 7. **Kryptosystem RSA i jego zastosowania** (kryptografia klucza publicznego, teoria liczb, implementacja RSA, testy pierwszości, algorytmy rozkładu na czynniki, ataki na RSA). 8. **Kryptografia klucza publicznego** (kryptosystem ElGamala, algorytmy dla problemu logarytmu dyskretnego, bezpieczeństwo algorytmów ElGamala). 9. **Sygnatury cyfrowe** (schemat podpisu RSA i ElGamala oraz jego warianty, funkcje skrótu o pełnej dziedzinie, certyfikaty, podpisywanie i szyfrowanie). 10. **Identyfikacja i uwierzytelnianie** (hasła, bezpieczne schematy identyfikacji dla kryptografii klucza tajnego i publicznego). 11. **Dystrybucja kluczy** (wstępna dystrybucja kluczy Diffiego-Hellmana, schemat Bloma, schemat dystrybucji klucza sesji). 12. **Metody uzgadniania klucza** (bezpieczeństwo warstwy transportu, uzgodnienie klucza Diffieg-Hellmana, funkcje wyprowadzania klucza, schematy MTI, zaprzeczalne schematy uzgadniania klucza, aktualizacja kluczy). 13. **Kryptografia post-kwantowa** (zastosowania kryptografii opartej na kratach NTRU, kryptosystem McEliece'a, schematy podpisu Lamporta, Winternitza i Merkle'a).

laboratorium	1. Wybrane algorytmy z zakresu podstaw kryptografii. 2. Implementacja klasycznych kryptosystemów. 3. Analiza wybranych współczesnych kryptosystemów. 4. Biblioteki programistyczne implementujące stosowane kryptosystemy i ich zastosowanie. 5. Implementacja wybranych algorytmów z zakresu kryptoanalizy liniowej, różnicowej i zintegrowanej.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01		x				
W02		x	x			
U01		x	x			
U02		x	x			
K01		x	x			

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	egzamin	Uzyskanie co najmniej 50% punktów z egzaminu
laboratorium	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					
		W	C	L	P	S	W	C	L	P	S	
1.	Udział w zajęciach zgodnie z planem studiów	**30**		**30**			**18**		**18**			h
2.	Inne (konsultacje, egzamin)	**4**		**2**			**4**		**2**			h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**66**					**42**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,64**					**1,68**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**59**					**83**					h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**2,36**					**3,32**					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**	**125**	**125**	h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**5**		ECTS

LITERATURA

1. Douglas R. Stinson, Maura Paterson, "Kryptografia w teorii i praktyce", Wydawnictwo naukowe PWN, Warszawa 2021.
2. W. Bray Shannon, "Algorytmy kryptograficzne w Pythonie Wprowadzenie", Wydawnictwo Helion, 2021.
3. Władysław Mochnacki, "Kody korekcyjne i kryptografia", Wydawnictwo PWr Wrocław, 2000.
4. Michael Wieschenbach, "Cryptography in C and C++ 2nd ed. Edition", Apress, 2013.
5. Gregory Bard: "Algebraic cryptoanalysis 2009th edition", Springer, 2009.