POLITECHNIKA BYDGOSKA
Wydział Inżynierii Mechanicznej

Karta przedmiotu

Kryptologia i systemy szyfrowania

1. Informacje podstawowe

Kierunek studiów technika bezpieczeństwa i obronności **Jednostka zarządzająca kierunkiem studiów** Wydział Inżynierii Mechanicznej **Poziom studiów** pierwszego stopnia (inż.) **Profil studiów** Profil ogólnoakademicki **Forma studiów** studia stacjonarne	**Cykl kształcenia (nabór)** 2024/25 **Kod przedmiotu** 03TBOS.PICC.2878.24 **Języki wykładowe** polski **Obligatoryjność** Obowiązkowy **Blok zajęciowy** Przedmioty kierunkowe

Wymagania wstępne	
Przedmioty wprowadzające	
Koordynator	Krzysztof Nowicki

Okres Semestr 3	**Forma zaliczenia** Egzamin **Forma prowadzenia i godziny zajęć** Wykład: 30 Ćwiczenia laboratoryjne: 15	**Liczba punktów ECTS** 4.0

Okres Semestr 4	**Forma zaliczenia** Zaliczenie na ocenę **Forma prowadzenia i godziny zajęć** Ćwiczenia laboratoryjne: 15 Ćwiczenia projektowe: 30	**Liczba punktów ECTS** 4.0

2. Efekty uczenia się dla przedmiotu

Kod	Opis efektów uczenia się	Odniesienie do kierunkowych efektów uczenia się	Odniesienie do charakterystyk PRK
Wiedza:			
W1	Ma ogólną wiedzę na temat stosowania kryptografii w obszarze cyberbezpieczeństwa. Posiada wiedzę w stopniu zaawansowanym dotyczącą algorytmów stosowanych w kryptografii i systemach szyfrowania.	TBO_O1_K_W08, TBO_O1_K_W09	P6S_WG, P6S_WG_inż, P6S_WG P6S_WG_inż
Umiejętności:			
U1	Potrafi dokonać wyboru i zastosować wybrane algorytmy szyfrowania i techniki kryptograficzne. Potrafi sformułować i ocenić rozwiązania z zakresu projektowania oraz implementacji algorytmów szyfrowania do zapewnienia bezpieczeństwa infrastruktury technicznej.	TBO_O1_K_U06, TBO_O1_K_U07	P6S_UW, P6S_UW_inż, P6S_UW P6S_UU P6S_UW_inż
Kompetencje społeczne:			
K1	Rozumie zasady współpracy i wymiany informacji z osobami o innych specjalnościach w kontekście zapewnienia integralności danych i metod komunikacji w systemie bezpieczeństwa.	TBO_O1_K_K05	P6S_KK

3. Treści programowe

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
1.	Całosemestralny projekt: W ramach tej formy zajęć studenci realizują całosemestralne prace praktyczne na zadane przez prowadzącego tematy.	Ćwiczenia projektowe	U1, K1

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
2.	Kryptologia, kryptografia i kryptoanaliza - podstawowe terminy. Funkcja kryptografii w informatyce i cyberbezpieczeństwie. Różne rodzaje kryptografii: z kluczem tajnym, z kluczem publicznym, bez klucza. Pojęcie prymitywu kryptograficznego. Historia kryptografii. Szyfry historyczne: monoalfabetyczne i poliafabetyczne. Maszyny szyfrujące: Enigma, maszyna Lorentza, szyfr Vernama. Zasada Kerkhoffsa. Bezpieczeństwo systemów kryptograficznych: sposoby definiowania i weryfikacji. Różne typy ataków kryptograficznych. Podstawy kryptoanalizy. Modele teoretyczne kryptosystemów. Siła algorytmu kryptograficznego. Teoria informacji Shannona. Szyfry z kluczem tajnym - ogólna budowa i zasada działania. Szyfry strumieniowe - ogólna zasada działania i wybrane przykłady realizacji. Szyfry blokowe. Podstawowe elementy składowe szyfru blokowego. Środowisko pracy szyfru blokowego: tryby pracy oraz dopełnienia. Budowa szyfru DES. Podstawy teoretyczne działania szyfru AES. Budowa AES i funkcje jego elementów składowych. Przegląd szyfrów blokowych: FEAL, Blowfish, Twofish, Camellia, etc. Szyfry blokowe wersus szyfry strumieniowej. Bezpieczeństwo szyfrów blokowych. Kryptografia z kluczem publicznym. Podstawy matematyczne: ciała skończone, problem faktoryzacji liczba całkowitych, problem logarytmu dyskretnego, krzywe eliptyczne. Elementy teorii złożoności obliczeniowej. Kryptosystem RSA i ElGamala. Protokół Diffiego-Hellmana. Podpis cyfrowy. Kryptografia krzywych eliptycznych. Pojęcie integralności danych. Funkcje skrótu (digest functions) i ich własności. Wybrane funkcji skrótu, ich budowa i własności. Kody uwierzytelniania wiadomości (MAC). Funkcje wyprowadzania klucza. Podstawy kryptoanalizy kwantowej. Wady i zalety komputerów kwantowych. Kryptografia postkwantowa. Podstawy teoretyczne i budowa wybranych algorytmów kryptografii postkwantowej. Szyfrowanie homomorficzne. Podstawy teoretyczne i konstrukcje wybranych schematów. Podstawy kryptografii kwantowej. Protokoły wymiany klucza: Bennetta-Brassarda, Eckarta etc. Szyfrowanie kwantowe.	Wykład	W1, K1

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
3.	W trakcie zajęć laboratoryjnych wykonywane będą ćwiczenia praktyczne mające na celu ugruntowanie wiedzy i pozyskanie umiejętności praktycznych w zakresie kryptografii: 1. Cel szyfrowania. Bezpieczeństwo szyfrowania. Szyfry XOR. Wykorzystanie generatorów liczb pseudolosowych w kryptografii 2. Szyfry strumieniowe - ogólna budowa. Realizacja szyfru opartego o rejestr przesuwający. 3. Szyfry blokowe z kluczem tajnym - implementacja typowego szyfru blokowego. 4. Szyfr AES - budowa i sposób implementacji operacji składowych. Implementacja szyfru w języku Python. 5. Środowisko pracy szyfru blokowego - dopełnienia i tryby pracy. Wektor IV i wartość nonce. 6. Kryptosystem z kluczem publiczny. Implementacja algorytmu RSA. Generowanie liczb pierwszych - test Rabina-Millera. Algorytm szybkiego potęgowania. 7. Funkcja skrótu. Implementacja funkcji skrótu opartej o schemat Damgarda-Merkla. 8. Kryptografia w praktyce. Standard OpenPGP. Narzędzie GnuPG. Szyfrowanie i podpisywanie dokumentów elektronicznych. Infrastruktura klucza publicznego.	Ćwiczenia laboratoryjne	U1, K1

4. Metody prowadzenia zajęć, weryfikacji efektów uczenia się i warunki zaliczenia

Semestr 3

Forma zajęć		
Wykład	**Metody prowadzenia zajęć:**	
	Wykład, Case study	
	Metody (sposoby) weryfikacji:	**Udział:**
	Zaliczenie pisemne	100%
	Warunki zaliczenia przedmiotu:	
	Wynik zaliczenia powyżej 50%	
Ćwiczenia laboratoryjne	**Metody prowadzenia zajęć:**	
	Ćwiczenia laboratoryjne	
	Metody (sposoby) weryfikacji:	**Udział:**
	Raport	100%
	Warunki zaliczenia przedmiotu:	
	Sprawozdania z ćwiczeń laboratoryjnych - komplet + 50% poprawność treści raportu.	

Semestr 4

Forma zajęć	

Ćwiczenia laboratoryjne	**Metody prowadzenia zajęć:**	
	Ćwiczenia laboratoryjne	
	Metody (sposoby) weryfikacji:	**Udział:**
	Raport	100%
	Warunki zaliczenia przedmiotu:	
	Sprawozdania z ćwiczeń laboratoryjnych - komplet + 50% poprawność treści raportu.	
Ćwiczenia projektowe	**Metody prowadzenia zajęć:**	
	Projekt	
	Metody (sposoby) weryfikacji:	**Udział:**
	Projekt	100%
	Warunki zaliczenia przedmiotu:	
	Przygotowanie dokumentacji projektowej - ocena powyżej 2,95	

Efekt uczenia się dla przedmiotu	**Metody (sposoby) weryfikacji**		
	Zaliczenie pisemne	Raport	Projekt
W1	x		
U1		x	x
K1	x	x	x

5. Literatura

Literatura podstawowa

1. Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, J.P. Aumasson, PWN 2018.
2. Kryptografia. W teorii i praktyce, Douglas R. Stinson, Helion, 2021

Literatura uzupełniająca

1. Teoria liczb w praktyce, Song Y. Yan, PWN, 2006.

6. Nakład pracy studenta - bilans godzin i punktów ECTS

Aktywność studenta		Obciążenie studenta Liczba godzin
Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia	Wykład	30
	Ćwiczenia laboratoryjne	30
	Ćwiczenia projektowe	30

Praca własna studenta	Przygotowanie do zajęć	45
	Studiowanie literatury	30
	Inne (przygotowanie do egzaminu)	20
	Konsultacje	15
Łączny nakład pracy studenta		200
Liczba punktów ECTS		8

* Godzina (dydaktyczna) oznacza 45 minut