KARTA KURSU

Nazwa	**Kryptografia kwantowa**
Nazwa w j. ang.	Quantum Cryptography

Koordynator	dr hab. prof. UP Piotr Czerski	Zespół dydaktyczny
		Zespół dydaktyczny: dr hab. prof. UP Piotr Czerski
Punktacja ECTS*	st. stacjonarne: 1 st. niestacjonarne: 1	

Opis kursu (cele kształcenia)

Celem przedmiotu jest przekazanie podstawowej wiedzy związanej z technikami gwarantowania poufności i integralności danych w systemach transmisji informacji oraz systemach komputerowych. Szczególny nacisk położony jest na metody kryptografii kwantowej. Kurs jest prowadzony w języku polskim.

Warunki wstępne

Wiedza	Znajomość podstaw algebry liniowej i analizy matematycznej. Podstawy teorii liczb, teorii informacji oraz teorii złożoności obliczeniowej.
Umiejętności	Umiejętność krytycznego myślenia
Kursy	Teoretyczne podstawy informatyki, Podstawy programowania, Sieci komputerowe.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student:	
	W01: zna klasyczne koncepcje kryptograficzne m.in. szyfry monoalfabetyczne, polialfabetyczne, XOR, schemat Vernama.	K_W01
	W02: omawia wybrane algorytmy gwarantowania poufności i integralności danych.	K_W01, K_W15
	W03: wymienia standardowe algorytmy szyfrowania danych.	K_W01

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student:	
	U01: rozumie dlaczego przetwarzanie informacji na poziomie kwantowym jest kluczowe dla bezpieczeństwa transmisji danych.	K_U01
	U02: rozumie idee kubitu i jego realizację w postaci bramek kwantowych.	K_U14
	U03: objaśnia zasady funkcjonowania infrastruktury klucza publicznego.	K_U17
	U04: charakteryzuje standardowe algorytmy szyfrowania danych.	K_U17

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student: K01: potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania. K02: rozumie potrzebę kształcenia ustawicznego i śledzenia na bieżąco zmian w zakresie standardów odnoszących się nowoczesnych algorytmów szyfrujących.	K_K03 K_K01

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A	K	L	S	P	E				
Liczba godzin	15										

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A	K	L	S	P	E				
Liczba godzin	10										

Opis metod prowadzenia zajęć

Podczas wykładów preferowane są metody aktywizujące i motywujące: metody dyskusji, intuicyjne przedstawianie pojęć abstrakcyjnych oraz historyczne sytuacje problemowe, które doprowadziły do wyłonienia się danej koncepcji lub teorii; motywujące są wzmianki o zastosowaniach fizycznych poszczególnych pojęć.

Formy sprawdzania efektów kształcenia

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01								X					
W02								X					
W03								X					
U01								X					
U02								X					
U03								X					
U04								X					
K01													
K02													

Kryteria oceny	Ocena końcowa jest zależna od aktywnego udziału w dyskusjach oraz systematyczności realizowanych zadań. Ocenę dobrą i bardzo dobrą może uzyskać student, który: • zna specyfikę kryptografii kwantowej. • objaśnia i implementuje algorytmy kryptografii. • orientuje się w podstawowych problemach i wyzwaniach nowoczesnej kryptografii.

Uwagi	

Treści merytoryczne (wykaz tematów)

1. Klasyczne koncepcje kryptograficzne m.in. szyfry monoalfabetyczne, polialfabetyczne, XOR.
2. Algorytmy gwarantowania poufności i integralności danych.
3. Funkcjonowanie infrastruktury klucza publicznego.
4. Mechanizmy tworzenia sygnatur cyfrowych, autoryzacji stron oraz protokoły współdzielenia informacji i przekazywania istotnych danych.
5. Standardowe algorytmy szyfrowania danych i systemów plików.
6. Algorytmy wykorzystywane w steganografii.
7. Metody stosowane w kryptografii kwantowej.

Wykaz literatury podstawowej

Wybrane rozdziały:

1. M. Karbowski, Podstawy kryptografii. Wydanie III, Helion 2014
2. Michel Le Bellac „Wstęp do informatyki kwantowej” PWN 2011
3. Stephen M. Barnett „Quantum Information.” Oxford University Press 2009

Wykaz literatury uzupełniającej

1. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii, Gliwice, Helion, 2012
2. Michael A. Nielsen & Isaac L. Chuang “Quantum Computation and Quantum Information” Cambridge. 2010

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **– studia stacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	15
	Opracowanie zadań domowych i referatu/prezentacji po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu (praca indywidualna lub w grupie)	
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		35
Liczba punktów ECTS w zależności od przyjętego przelicznika		1

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **– studia niestacjonarne**

Liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Opracowanie zadań domowych i referatu/prezentacji po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu (praca indywidualna lub w grupie)	
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		35
Liczba punktów ECTS w zależności od przyjętego przelicznika		1