KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Teoria liczb i elementy kryptografii	**1010341661010348732**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Matematyka	**(brak)**	**3 / 6**
Ścieżka obieralności/specjalność	**Przedmiot oferowany w języku:**	**Kurs (obligatoryjny/obieralny)**
Modelowanie matematyczne	**polski**	**obligatoryjny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
I stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **30** Ćwiczenia: **-** Laboratoria: **30** Projekty/seminaria: **-**	**4**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny)	(ogólnouczelniany, z innego kierunku)
(brak)	**(brak)**

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**

Odpowiedzialny za przedmiot / wykładowca:

dr Anna Iwaszkiewicz-Rudoszańska
email: anna.iwaszkiewicz-rudoszanska@put.poznan.pl
tel. 61 665 2812
Wydział Elektryczny
ul. Piotrowo 3A, 60-965 Poznań

Odpowiedzialny za przedmiot / wykładowca:

dr Piotr Rejmenciak
email: piotr.rejmenciak@put.poznan.pl
tel. 61 665 2359
Wydział Elektryczny
ul. Piotrowo 3A, 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Podstawowe wiadomości z zakresu algebry.
2	**Umiejętności:**	Umiejętność przeprowadzania poprawnych wnioskowań logicznych.
3	**Kompetencje społeczne**	Rozumienie konieczności poszerzania swoich kompetencji.

Cel przedmiotu:

Zapoznanie tą częścią teorii liczb, która jest potrzebna do zrozumienia podstawowych schematów kryptografii z kluczem publicznym. Przedstawienie podstawowych algorytmów i praktycznych zastosowań kryptografii z kluczem publicznym.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Wykazywanie własności relacji podzielności i przystawania modulo n. - [K_W04]
2. Objaśnianie idei kryptografii z kluczem publicznym i wskazanie przykłów takich kryptosystemów. - [K_W01]

Umiejętności:

1. Wykorzystywanie kongruencji do rozwiązywać równań diofantycznych. - [K_U01]
2. Wykonywanie obliczeń niezbędne do szyfrowania opartego na problemie logarytmu dyskretnego w grupie multiplikatywnej ciała skończonego i grupie punktów na krzywej eliptycznej. - [K_U05, K_U17]
3. Wykorzystywanie twierdzeń z teorii liczb i algebry w analizie systemów kryptograficznych. Uzasadnianie poprawności działania wybranych systemów kryptograficznych - [K_U01, K_U36]

Kompetencje społeczne:

1. Znajomość ograniczeń współczesnej kryptografii - [K_K07]

Sposoby sprawdzenia efektów kształcenia

Wykład

Ocena wiedzy i umiejętności wykazanych na egzaminie pisemnym i ustnym.

Laboratoria

Premiowanie wiedzy niezbędnej do realizacji postawionych problemów w danym obszarze ćwiczeń.

Ocenianie ciągłe, na każdych zajęciach - premiowanie przyrostu umiejętności posługiwania się poznanymi zasadami i metodami.

Dwa kolokwia (student może wówczas korzystać z przygotowanych notatek i materiałów wykładowych).

Rozwiązywanie problemowych zadań domowych.

Treści programowe

Teoria podzielności w pierścieniu liczb całkowitych. Algorytm Euklidesa. Liczby pierwsze. Kongruencje, cechy podzielności (także w systemach liczbowych o dowolnej podstawie), kongruencje liniowe, liniowe równania diofantyczne. Chińskie twierdzenie o resztach, małe twierdzenie Fermata, funkcja Eulera i jej własności, twierdzenie Eulera. Kongruencje kwadratowe, reszty kwadratowe, symbol Legendre?a i Jacobiego, prawo wzajemności reszt kwadratowych. Faktoryzacja liczb całkowitych. Testy pierwszości. Problem logarytmu dyskretnego. Protokół uzgadniania kluczy Diffiego-Hellmana. Systemy kryptograficzne z kluczem publicznym ? RSA, Rabina i ElGamala. Podpisy cyfrowe RSA i ElGamala. Ślepe podpisy, kanał podprogowy. Krzywe eliptyczne nad dowolnymi ciałami. Działania na punktach krzywych eliptycznych. Krzywe eliptyczne nad ciałami skończonymi. Systemy kryptograficzne używające krzywych eliptycznych. Złożoność obliczeniowa algorytmów teorio-liczbowych.

Literatura podstawowa:

1. N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa 1995

2. W. Marzantowicz, P. Zarzycki, Elementarna teoria liczb, PWN Warszawa 2006

3. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2005

Literatura uzupełniająca:

1. W. Narkiewicz, Teoria liczb, PWN Warszawa 2003

2. M. Kutyłowski, W. Strothmann, Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Wydawnictwo READ ME, 1999

3. W. Sierpiński, Teoria liczb, MM tom 19, IM PAN, Warszawa 1950

4. D.R. Stinson, Kryptografia w teorii i w praktyce, WNT, Warszawa 2005

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	90	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2
Zajęcia o charakterze praktycznym	30	2