KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Teoria liczb i elementy kryptografii	

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Matematyka w technice	**ogólnoakademicki**	**3 / 6**

Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
Modelowanie w technice	**polski**	**obieralny**

Stopień studiów:	**Forma studiów (stacjonarna/niestacjonarna)**
I stopień (poziom PRK 6)	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **15** Ćwiczenia: **15** Laboratoria: Projekty/seminaria: **-**	**2**

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

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**2 100%**
nauki techniczne	**2 100%**

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:

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Podstawowe wiadomości z zakresu algebry i matematyki dyskretnej. [K_W01 (P6S_WG)]
2	**Umiejętności:**	Umiejętność przeprowadzania poprawnych wnioskowań logicznych. [K_U01 (P6S_UW), K_U02 (P6S_UW)]
3	**Kompetencje społeczne**	Rozumienie konieczności poszerzania swoich kompetencji. [K_K01 (P6S_KK), K_K02 (P6S_KK)]

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. Zna pojęcia i twierdzenia z teorii liczb wykorzystywane w omawianych algorytmach kryptograficznych. – [K_W01 (P6S_WG)]
2. Wyjaśnia ideę kryptografii z kluczem publicznym , wskazuje przykłady takich kryptosystemów. – [K_W06 (P6S_WG)]

Umiejętności:

1. Wykonuje obliczenia niezbędne do szyfrowania i deszyfrowania w omawianych systemach kryptograficznych. – [K_U03 (P6S_WG), K_U04 (P6S_UW)]
2. Wykorzystuje twierdzenia z teorii liczb i algebry w analizie systemów kryptograficznych. Uzasadnia poprawności działania wybranych systemów kryptograficznych. – [K_U01 (P6S_UW), K_U03 (P6S_UW)]

Kompetencje społeczne:

1. Rozumie konieczność dalszego samokształcenia. – [K_K02 (P6S_KK)]
2. Ma świadomość ograniczeń współczesnej kryptografii. – [K_K01 (P6S_KK)]

Sposoby sprawdzenia efektów kształcenia

Wykład

Ocena wiedzy i umiejętności wykazanych na zaliczeniu pisemnym wykładu.

Ćwiczenia

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 sprawdziany.
Rozwiązywanie problemowych zadań domowych.

Treści programowe

Przypomnienie wiadomości dotyczących kongruencji (chińskie twierdzenie o resztach, małe twierdzenie Fermata, funkcja Eulera i twierdzenie Eulera). Kongruencje kwadratowe, reszty kwadratowe, symbol Legendre'a i Jacobiego, prawo wzajemności reszt kwadratowych. 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.
Aktualizacja:28.10.2018

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. W. Sierpiński, Teoria liczb, MM tom 19, IM PAN, Warszawa 1950.
3. D.R. Stinson, kryptografia w teorii i w praktyce, WNT, Warszawa 2005

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Udział w zajęciach wykładowych	15
2. Udział w zajęciach ćwiczeniowych	15
3. Udział w konsultacjach związanych z realizacją procesu kształcenia	4
4. Przygotowanie do ćwiczeń/ćwiczeń laboratoryjnych	15
5. Przygotowanie do sprawdzianów / kolokwium	6
6. Przygotowanie do zaliczenia wykładu	5

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	60	2
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	34	1
Zajęcia o charakterze praktycznym	15	1