# KARTA PRZEDMIOTU

| | | |
|---|---|---|
| **Kod przedmiotu** | 0541-2MAT-F61-PK | |
| **Nazwa przedmiotu w języku** | polskim | ***Podstawy kryptografii*** |
| | angielskim | ***The basics of cryptography*** |

## 1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

| | |
|---|---|
| **1.1. Kierunek studiów** | matematyka |
| **1.2. Forma studiów** | studia stacjonarne |
| **1.3. Poziom studiów** | studia pierwszego stopnia, licencjackie |
| **1.4. Profil studiów** | ogólnoakademicki |
| **1.5. Specjalność** | nauczanie matematyki, zastosowania matematyki |
| **1.6. Jednostka prowadząca przedmiot** | WM, Instytut Matematyki |
| **1.7. Osoba/zespół przygotowująca/y kartę przedmiotu** | prof. zw. dr hab. Taras Banakh, prof. UJK dr hab. Andrzej Chrzęszczyk, dr Joanna Garbulińska-Węgrzyn, |
| **1.8. Osoba odpowiedzialna za przedmiot** | |
| **1.9. Kontakt** | |

## 2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

| | |
|---|---|
| **2.1. Przynależność do modułu** | Fakultatywny |
| **2.2. Język wykładowy** | polski |
| **2.3. Semestry, na których realizowany jest przedmiot** | 6 |
| **2.4. Wymagania wstępne** | Algebra z teorią liczb |

## 3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

| | | |
|---|---|---|
| **3.1. Forma zajęć** | | wykład, ćwiczenia laboratoryjne |
| **3.2. Miejsce realizacji zajęć** | | zajęcia w pomieszczeniu dydaktycznym UJK |
| **3.3. Forma zaliczenia zajęć** | | zaliczenie z oceną (wykład), zaliczenie z oceną (ćwiczenia laboratoryjne) |
| **3.4. Metody dydaktyczne** | | wykład - wykład, dyskusja, praca z książką<br>ćwiczenia laboratoryjne – dyskusja, rozwiązywanie zadań, praca z książką |
| **3.5. Wykaz literatury** | **podstawowa** | Chrzęszczyk A., Algorytmy teorii liczb i kryptografii. BTC. Legionowo 2010<br>Koblitz N., Wykład z teorii liczb i kryptografii. WNT. Warszawa 1995 |
| | **uzupełniająca** | Koblitz N., Algebraiczne aspekty kryptografii. WNT. Warszawa 2000<br>Menezes A. J. i in., Kryptografia stosowana. WNT. Warszawa 2005<br>Stinson D. R., Kryptografia w teorii i praktyce. WNT. Warszawa 2005 |

## 4. CELE, TREŚCI I EFEKTY KSZTAŁCENIA

**4.1. Cele przedmiotu** ***(z uwzględnieniem formy zajęć)***

***Wykład***

C1 – zapoznanie z podstawowymi metodami stosowanymi w kryptografii

***Ćwiczenia laboratoryjne***

C1 – rozwijanie umiejętności implementacji algorytmów i zastosowania zdobytej wiedzy z wykorzystaniem pakietów obliczeniowych

C2 – kształtowanie rozumienia potrzeby ciągłego uczenia się

**4.2. Treści programowe** ***(z uwzględnieniem formy zajęć)***

***Wykład specjalnościowy:***

Rozwinięcia liczb przy danej podstawie. Kodowanie tekstu przy pomocy liczb. Szyfry symetryczne, wkład matematyków polskich w złamanie Enigmy. Kryptosystem RSA. Konstruowanie ciał skończonych. Efektywna arytmetyka w ciałach skończonych.. Problem logarytmu dyskretnego w ciałach skończonych. Schemat wymiany kluczy Diffiego-Hellmana, Kryptosystem ElGamala, podpisy cyfrowe. Zastosowania krzywych eliptycznych w kryptografii.

***Ćwiczenia laboratoryjne:***

Rozwinięcia liczb przy danej podstawie, kodowanie tekstu przy pomocy liczb. Przykłady szyfrowania symetrycznego. Szyfrowanie RSA. Konstruowanie ciał skończonych. Efektywna arytmetyka w ciałach skończonych. Kryptosystem ElGamala, podpisy cyfrowe. Rozwiązywania problemu logarytmu dyskretnego. Wykorzystanie krzywych eliptycznych. Zapisywanie algorytmów w pseudokodzie i implementacja wybranym języku programowania. Wykorzystanie pakietów obliczeniowych.

### 4.3. Przedmiotowe efekty kształcenia

| Efekt | Student, który zaliczył przedmiot | Odniesienie do kierunkowych efektów kształcenia |
|---|---|---|
| w zakresie **WIEDZY:** | | |
| W01 | rozumie cywilizacyjne znaczenie matematyki i jej zastosowań w kryptografii | MAT1A_W01 |
| W02 | definiuje podstawy technik obliczeniowych programowania, wspomagających pracę matematyka i rozumie ich ograniczenia | MAT1A_W08<br>MAT1A_W16 |
| W03 | posługuje się na poziomie podstawowym co najmniej jednym pakietem oprogramowania służącym do obliczeń symbolicznych (Magma lub Sage) | MAT1A_W09 |
| w zakresie **UMIEJĘTNOŚCI:** | | |
| U01 | tworzy ciała skończone drogą konstruowania pierścieni ilorazowych | MAT1A_U02 |
| U02 | dostrzega obecność i rolę struktur algebraicznych w kryptografii (np. ciał skończonych) | MAT1A_U11 |
| U03 | rozpoznaje problemy związane z szyfrowaniem, które można rozwiązać algorytmicznie | MAT1A_U15 |
| U04 | planuje swoją pracę | MAT1A_U26 |
| U05 | pracuje w grupie, współpracuje z jej członkami w celu opracowania złożonych algorytmów. | MAT1A_U27 |
| w zakresie **KOMPETENCJI SPOŁECZNYCH:** | | |
| K01 | precyzyjnie formułuje pytania służące pogłębieniu własnego zrozumienia danego tematy lub odnalezieniu brakujących elementów rozumowania | MAT1A_K01 |

### 4.4. Sposoby weryfikacji osiągnięcia przedmiotowych efektów kształcenia

| Efekty przedmiotowe *(symbol)* | Sposób weryfikacji (+/-) | | | |
|---|---|---|---|---|
| | Kolokwium | | Zadania domowe | |
| | *Forma zajęć* | | *Forma zajęć* | |
| | *W* | *C* | *W* | *C* |
| W01 | + | | | |
| W02 | + | | | |
| W03 | + | | | |
| U01 | | + | | + |
| U02 | | + | | + |
| U03 | | + | | + |
| U04 | | + | | + |
| U05 | | + | | + |
| K01 | | | | |

### 4.5. Kryteria oceny stopnia osiągnięcia efektów kształcenia

| Forma zajęć | Ocena | Kryterium oceny |
|---|---|---|
| wykład (*W*) | **3** | co najmniej 50% i nie więcej, niż 60% łącznej liczby punktów możliwych do uzyskania |
| | **3,5** | ponad 60% i nie więcej, niż 70% łącznej liczby punktów możliwych do uzyskania |
| | **4** | ponad 70% i nie więcej, niż 80% łącznej liczby punktów możliwych do uzyskania |
| | **4,5** | ponad 80% i nie więcej, niż 90% łącznej liczby punktów możliwych do uzyskania |
| | **5** | ponad 90% liczby punktów możliwych do uzyskania |
| ćwiczenia laboratoryjne (*C*) | **3** | co najmniej 50% i nie więcej, niż 60% łącznej liczby punktów możliwych do uzyskania |
| | **3,5** | ponad 60% i nie więcej, niż 70% łącznej liczby punktów możliwych do uzyskania |
| | **4** | ponad 70% i nie więcej, niż 80% łącznej liczby punktów możliwych do uzyskania |
| | **4,5** | ponad 80% i nie więcej, niż 90% łącznej liczby punktów możliwych do uzyskania |
| | **5** | ponad 90% liczby punktów możliwych do uzyskania |

**5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA**

| Kategoria | Obciążenie studenta |
|---|---|
| | **Studia stacjonarne** |
| *LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/* | ***64*** |
| *Udział w wykładach* | 30 |
| *Udział w ćwiczeniach laboratoryjnych* | 30 |
| *Udział w kolokwium zaliczeniowym* | 4 |
| *SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/* | ***61*** |
| *Przygotowanie do wykładu* | 10 |
| *Przygotowanie do ćwiczeń laboratoryjnych* | 31 |
| *Przygotowanie do egzaminu/kolokwium* | 20 |
| ***ŁĄCZNA LICZBA GODZIN*** | ***125*** |
| **PUNKTY ECTS za przedmiot** | **5** |

***Przyjmuję do realizacji*** *(data i podpisy osób prowadzących przedmiot w danym roku akademickim)*

.....