

# POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2020/2021

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: M

Stopień studiów: II

Specjalności: Modelowanie matematyczne

### 1 INFORMACJE O PRZEDMIOCIE

|                                         |                                       |
|-----------------------------------------|---------------------------------------|
| NAZWA PRZEDMIOTU                        | Matematyczne podstawy kryptologii     |
| NAZWA PRZEDMIOTU<br>W JĘZYKU ANGIELSKIM | Mathematical foundation of cryptology |
| KOD PRZEDMIOTU                          | WiT M oIIS C10 20/21                  |
| KATEGORIA PRZEDMIOTU                    | Przedmioty kierunkowe                 |
| LICZBA PUNKTÓW ECTS                     | 7.00                                  |
| SEMESTRY                                | 3                                     |

### 2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM<br>KOMPUTERO-<br>WE | SEMINARIUM | PROJEKT |
|---------|--------|-----------|--------------|----------------------------------|------------|---------|
| 3       | 30     | 30        | 0            | 0                                | 0          | 0       |

### 3 CELE PRZEDMIOTU

**Cel 1** Nacyzyć studentów matematycznych podstaw i metod współczesnej kryptologii

## 4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- 1 Algebra liniowa z geometrią analityczną, podstawy algebry abstrakcyjnej, elementy analizy matematycznej, elementy teorii liczb oraz logika i matematyka dyskretna

## 5 EFEKTY KSZTAŁCENIA

**EK1 Wiedza** Student zna podstawowe pojęcia teorii liczb, niezbędne w kryptologii, demonstruje jak zaszyfrować i deszyfrować informację za pomocą pewnych szyfrów klasycznych i współczesnych, lecz również

**EK2 Wiedza** Student zna podstawy teorii Shannona (pojęcia oraz twierdzenia) o szyrowaniu i bezpieczeństwie informacji oraz kryptografię klasyczną, podstawy szyfrowania symetrycznego i asymetrycznego.

**EK3 Kompetencje społeczne** Student potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze, także w językach obcych.

**EK4 Umiejętności** Student wie i demonstruje jak zrealizować szyrowanie i deszyfrowanie za pomocą podstawowych szyfrów.

## 6 TREŚCI PROGRAMOWE

| WYKŁAD    |                                                                                                                                                                                                                                                                                                                         |                  |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| LP        | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                                                                                                                                                                                                                                                  | LICZBA<br>GODZIN |
| <b>W1</b> | Elementy kryptologii: Ochrona danych, systemy i algorytmy kryptograficzne, własności informacyjne języka                                                                                                                                                                                                                | 2                |
| <b>W2</b> | Elementy teorii liczb: twierdzenie o dzieleniu z resztą, podzielność, klasy reszt modulo $n$ , rozszerzony algorytm Euklidesa, NWD, NWW, liczby względnie pierwsze, zasadnicze twierdzenie arytmetyki, twierzenie Euklidesa o liczbach pierwszych, sito Eratostenesa, funkcje arytmetyczne, twierzenia Eulera i Fermata | 8                |
| <b>W3</b> | Obliczeniowa i algorytmiczna teoria liczb: testy pierwszości, algorytmy faktoryzacji liczb całkowitych, logarytmy dyskretne, generowanie liczb pierwszych                                                                                                                                                               | 4                |
| <b>W4</b> | Kryptografia klasyczna: proste szyfry podstawieniowe, szyfry podstawieniowe homofoniczne, szyfry podstawieniowe wieloalfabetowe, szyfry podstawieniowe poligramowe, szyfry przestawieniowe                                                                                                                              | 4                |
| <b>W5</b> | Szyfry symetryczne                                                                                                                                                                                                                                                                                                      | 4                |
| <b>W6</b> | Bezpieczeństwo informacji, algorytm DES                                                                                                                                                                                                                                                                                 | 2                |
| <b>W7</b> | Szyfry asymetryczne                                                                                                                                                                                                                                                                                                     | 4                |
| <b>W8</b> | Podpisy cyfrowe                                                                                                                                                                                                                                                                                                         | 2                |

| ĆWICZENIA |                                                                                                                                                                                                                                                                                                                                                   |                  |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| LP        | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                                                                                                                                                                                                                                                                            | LICZBA<br>GODZIN |
| <b>C1</b> | Wstęp do kryptologii: Ochrona danych, systemy i algorytmy kryptograficzne, własności informacyjne języka                                                                                                                                                                                                                                          | 2                |
| <b>C2</b> | Ćwiczenia z podstawowych zagadnień teorii liczb: twierdzenie o dzieleniu z resztą, podzielność, klasy reszt modulo $n$ , rozszerzony algorytm Euklidesa, NWD, NWW, liczby względnie pierwsze, zasadnicze twierdzenie arytmetyki, twierzenie Euklidesa o liczbach pierwszych, sito Eratostenesa, funkcje arytmetyczne, twierzenia Eulera i Fermata | 8                |
| <b>C3</b> | Testy pierwszości, algorytmy faktoryzacji liczb całkowitych, logarytmy dyskretne, generowanie liczb pierwszych                                                                                                                                                                                                                                    | 4                |
| <b>C4</b> | Rozwiązywanie zadań z kryptografii klasycznej: proste szyfry podstawieniowe, szyfry podstawieniowe homofoniczne, szyfry podstawieniowe wieloalfabetowe, szyfry podstawieniowe poligramowe, szyfry przestawieniowe                                                                                                                                 | 4                |
| <b>C5</b> | Badanie własności szyfrów symetrycznych                                                                                                                                                                                                                                                                                                           | 4                |
| <b>C6</b> | Omówienie problemów związanych z bezpieczeństwem informacji, algorytm DES                                                                                                                                                                                                                                                                         | 2                |
| <b>C7</b> | Przykłady szyfrów asymetrycznych                                                                                                                                                                                                                                                                                                                  | 4                |
| <b>C8</b> | Sposoby podpisów cyfrowych, przykłady                                                                                                                                                                                                                                                                                                             | 2                |

## 7 NARZĘDZIA DYDAKTYCZNE

**N1** Wykłady. W sytuacji zdalnego nauczania prowadzone są za pośrednictwem MS Teams, na żywo. e-Kurs na platformie Delta PK.

**N2** Praca w grupach. W sytuacji zdalnego nauczania prowadzone są za pośrednictwem MS Teams, na żywo.

**N3** Konsultacje

## 8 OBCIĄŻENIE PRACĄ STUDENTA

| FORMA AKTYWNOŚCI                                                                                 | ŚREDNIA LICZBA GODZIN<br>NA ZREALIZOWANIE<br>AKTYWNOŚCI |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Godziny kontaktowe z nauczycielem akademickim, w tym:</b>                                     |                                                         |
| Godziny wynikające z planu studiów                                                               | 60                                                      |
| Konsultacje przedmiotowe                                                                         | 30                                                      |
| Egzaminy i zaliczenia w sesji                                                                    | 15                                                      |
| <b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b> |                                                         |
| Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury                               | 75                                                      |
| Opracowanie wyników                                                                              | 30                                                      |
| Przygotowanie raportu, projektu, prezentacji, dyskusji                                           | 0                                                       |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z<br/>CAŁEGO NAKŁADU PRACY STUDENTA</b>    | <b>210</b>                                              |
| SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU                                                    | 7.00                                                    |

## 9 SPOSOBY OCENY

Aktywność w e-kursie umieszczonym na platformie Delta PK. W sytuacji zdalnego nauczania wszystkie sprawdziany prowadzone są za pośrednictwem platformy Delta PK i MS Teams.

### OCENA FORMUJĄCA

**F1** Kolokwium

**F2** Ćwiczenie praktyczne, obecność

### OCENA PODSUMOWUJĄCA

**P1** Egzamin pisemny

**P2** Egzamin ustne

### WARUNKI ZALICZENIA PRZEDMIOTU

**W1** obecność na zajęciach, ocena pozytywna na ćwiczeniach oraz ocena pozytywna na kolokwium oraz na egzaminach pisemnym i ustnym

### OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA

**B1** test

### KRYTERIA OCENY

| EFEKT KSZTAŁCENIA 1 |                                                                                                                                                                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 2.0        | Student nie zna podstawowe pojęcia z teorii liczb i szyfrowania, nie ilustruje ich przykładami                                                                                                                                                                            |
| NA OCENĘ 3.0        | Student zna podstawowe pojęcia z teorii liczb i szyfrowania, ilustruje ich przykładami                                                                                                                                                                                    |
| NA OCENĘ 3.5        | Student zna podstawowe pojęcia z teorii liczb i szyfrowania, może formułować podstawowe zagadnienia, ilustruje ich przykładami                                                                                                                                            |
| NA OCENĘ 4.0        | Student zna podstawowe pojęcia z teorii liczb i szyfrowania, może udowodnić podstawowe zagadnienia, ilustruje ich przykładami                                                                                                                                             |
| NA OCENĘ 4.5        | Student zna podstawowe pojęcia z teorii liczb i szyfrowania, ilustruje ich przykładami, może udowodnić podstawowe zagadnienia z teorii liczb i szyfrowania i stosować ich do rozwiązywania standardowych zadań teoretycznego i praktycznego charakteru                    |
| NA OCENĘ 5.0        | Student zna podstawowe pojęcia z teorii liczb i szyfrowania, ilustruje ich przykładami, może udowodnić podstawowe zagadnienia z teorii liczb i szyfrowania i stosować ich do rozwiązywania standardowych i niestandardowych zadań teoretycznego i praktycznego charakteru |
| EFEKT KSZTAŁCENIA 2 |                                                                                                                                                                                                                                                                           |
| NA OCENĘ 2.0        | Student nie zna podstawowe pojęcia teorii Shannona o szyfrowaniu oraz nie ilustruje ich przykładami                                                                                                                                                                       |
| NA OCENĘ 3.0        | Student zna podstawowe pojęcia teorii Shannona o szyfrowaniu oraz ilustruje ich przykładami                                                                                                                                                                               |
| NA OCENĘ 3.5        | Student zna podstawowe pojęcia i podstawowe zagadnienia teorii Shannona o szyfrowaniu, może, zilustrować przykładami oraz rozwiązywaniem zadań elementarnych                                                                                                              |
| NA OCENĘ 4.0        | Student zna podstawowe pojęcia i podstawowe zagadnienia teorii Shannona o szyfrowaniu, może udowodnić podstawowe zagadnienia, zilustrować przykładami oraz rozwiązywaniem zadań elementarnych                                                                             |
| NA OCENĘ 4.5        | Student zna podstawowe pojęcia i podstawowe zagadnienia teorii Shannona o szyfrowaniu, może udowodnić podstawowe zagadnienia i stosować ich do rozwiązywania standardowych zadań oraz ilustruje ich przykładami                                                           |
| NA OCENĘ 5.0        | Student zna podstawowe pojęcia teorii Shannona o szyfrowaniu, może udowodnić podstawowe zagadnienia i stosować ich do rozwiązywania standardowych i niestandardowych zadań teoretycznego i praktycznego charakteru                                                        |
| EFEKT KSZTAŁCENIA 3 |                                                                                                                                                                                                                                                                           |
| NA OCENĘ 2.0        | Student nie zna ograniczenia własnej wiedzy, nie potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego przedmiotu                                                                                                                       |
| NA OCENĘ 3.0        | Student zna ograniczenia własnej wiedzy, potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego przedmiotu                                                                                                                               |

|                     |                                                                                                                                                                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 3.5        | Student zna podstawowe pojęcia i podstawowe zagadnienia i może ich zilustrować                                                                                                                                                                                                  |
| NA OCENĘ 4.0        | Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, może ich zilustrować i udowodnić, rozumie konieczność systematycznej pracy                                                                                                                                   |
| NA OCENĘ 4.5        | Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, może ich zilustrować, udowodnić i rozwiązać podstawowe zadania, rozumie konieczność systematycznej pracy, potrafi samodzielnie wyszukiwać informacje w literaturze, także w językach obcych                  |
| NA OCENĘ 5.0        | Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, może ich zilustrować, udowodnić i rozwiązać podstawowe i niestandardowe zadania, rozumie konieczność systematycznej pracy, potrafi samodzielnie wyszukiwać informacje w literaturze, także w językach obcych |
| EFEKT KSZTAŁCENIA 4 |                                                                                                                                                                                                                                                                                 |
| NA OCENĘ 2.0        | Student nie zna podstawowe pojęcia, nie umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować podstawowe pojęcia przykładami                                                                                                                                  |
| NA OCENĘ 3.0        | Student zna podstawowe pojęcia, umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować podstawowe pojęcia przykładami                                                                                                                                          |
| NA OCENĘ 3.5        | Student zna podstawowe pojęcia i zagadnienia, umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować ich przykładami                                                                                                                                           |
| NA OCENĘ 4.0        | Student zna podstawowe pojęcia i zagadnienia z dowodami, umie rozwiązać podstawowe zadania praktycznego i teoretycznego charakteru i zilustrować ich przykładami                                                                                                                |
| NA OCENĘ 4.5        | Student zna podstawowe pojęcia, ich związki oraz zagadnienia z dowodami, umie rozwiązać zadania praktycznego i teoretycznego charakteru, zilustrować ich przykładami                                                                                                            |
| NA OCENĘ 5.0        | Student zna podstawowe pojęcia i podstawowe zagadnienia, ich związki oraz zagadnienia z dowodami, umie rozwiązać standardowe i niestandardowe zadania praktycznego i teoretycznego charakteru, zilustrować ich przykładami i stosować na praktyce                               |

## 10 MACIERZ REALIZACJI PRZEDMIOTU

| EFEKT KSZTAŁCENIA | ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU | CELE PRZEDMIOTU | TREŚCI PROGRAMOWE          | NARZĘDZIA DYDAKTYCZNE | SPOSOBY OCENY |
|-------------------|--------------------------------------------------------------------------------|-----------------|----------------------------|-----------------------|---------------|
| EK1               | K_W01 K_W02<br>K_W06 K_W07<br>K_K01                                            | Cel 1           | W1 W2 W4 C1<br>C2 C3 C4    | N1 N2 N3              | F1 F2 P1 P2   |
| EK2               | K_W01 K_W02<br>K_W08 K_U10<br>K_U11 K_K07                                      | Cel 1           | W5 W6 C5 C6                | N1 N2 N3              | F1 F2 P1 P2   |
| EK3               | K_U10 K_U15<br>K_K05 K_K06                                                     | Cel 1           | W5 W6 W7 W8<br>C5 C6 C7 C8 | N1 N2 N3              | F1 F2 P1 P2   |
| EK4               | K_U01 K_U02<br>K_U04 K_K06                                                     | Cel 1           | W7 W8 C7 C8                | N1 N2 N3              | F1 F2 P1 P2   |

## 11 WYKAZ LITERATURY

### LITERATURA PODSTAWOWA

- [1] | **N. Koblitz** — *Wykład z teorii liczb i kryptografii*, Warszawa, 1995, WNT
- [2] | **N. Koblitz** — *Algebraiczne aspekty kryptografii*, Warszawa, 2000, WNT
- [3] | **W. Mochnacki** — *Kody korekcyjne i kryptografia*, Wrocław, 1997, PolitechnikaWrocławska
- [4] | **Song Y. Yan** — *Teoria liczb w informatyce*, Warszawa, 2006, PWN

### LITERATURA UZUPEŁNIAJĄCA

- [1] | **J.A. Buchmann** — *Wprowadzenie do kryptografii*, Warszawa, 2006, PWN

## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

prof. dr hab. Orest Artemovych (kontakt: [artemo@pk.edu.pl](mailto:artemo@pk.edu.pl))

### OSOBY PROWADZĄCE PRZEDMIOT

- 1 Prof. dr hab. Orest Artemovych (kontakt: [artemo@usk.pk.edu.pl](mailto:artemo@usk.pk.edu.pl))

## 13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)



**PRZYJMUJĘ DO REALIZACJI** (data i podpisy osób prowadzących przedmiot)

.....