Nazwa przedmiotu
Algebraiczne podstawy kryptografii
Algebraic Foundations of Cryptography

Kod ECTS
3.1.KRK.12TY.AlPK

Nazwa jednostki prowadzącej przedmiot
Uniwersytet Opolski, Wydział Matematyki, Fizyki i Informatyki, Instytut Matematyki i Informatyki

Studia

Kierunek	stopień	tryb	specjalność	specjalizacja
Matematyka	*Drugi*	*Stacjonarne* *Niestacjonarne*[*)]		

Nazwisko osoby prowadzącej (osób prowadzących)
Pracownicy Zakładu Algebry

Formy zajęć, sposób ich realizacji i przypisana im liczba godzin

A. Formy zajęć
- *wykład*

B. Sposób realizacji
- *zajęcia w sali wykładowej*

C. Liczba godzin

Wykład – 30 godzin

*) Studia niestacjonarne:
Wykład – 18 godz. (2T+16Z)

Liczba punktów ECTS: 3

Bilans nakładu pracy przeciętnego studenta:
- *2 godz. – wstępny przegląd literatury [*) 2]*
- *15×2 godz. = 30 godz. – udział w wykładach [*) 18]*
- *15×2 godz. = 30 godz. – analiza i przyswojenie treści wykładu [*) 42]*
- *5× 1 godz. = 5 godz. – udział w konsultacjach do wykładu [*) 2]*
- *8 godz. – przygotowanie do egzaminu [*) 12]*
- *2 godz. – konsultacje przed egzaminem [*) 1]*
- *3 godz. – udział w egzaminie [*) 3]*

Łączny nakład pracy studenta: 80 godzin, co odpowiada 3 pkt. ECTS

w tym
- *nakład pracy związany z zajęciami wymagającymi bezpośredniego udziału nauczycieli akademickich: 30+5+2+3=**40** godz., co odpowiada **1,5** pkt. ECTS;*
- *nakład pracy związany z zajęciami o charakterze praktycznym: 8+3=**11** godz., co odpowiada **<0,5** pkt. ECTS*

*) na studiach niestacjonarnych:
- *nakład pracy związany z zajęciami wymagającymi bezpośredniego udziału nauczycieli akademickich: 18+2+1+3=**24** godz., co odpowiada **1** pkt. ECTS;*
- *nakład pracy związany z zajęciami o charakterze praktycznym: 12+3=**15** godz., co odpowiada **0,5** pkt ECTS*

Status przedmiotu
- *specjalnościowy/do wyboru*

Język wykładowy
Polski (możliwość realizacji w języku angielskim)

Metody dydaktyczne
- *wykład / wykład problemowy / wykład z prezentacją multimedialną*

Forma i sposób zaliczenia oraz podst. kryteria oceny lub wymagania egzaminacyjne
Na ogólnych zasadach określonych w programie kształcenia, a w szczególności

A. Sposób zaliczenia
- *egzamin na ocenę*

B. Formy zaliczenia
- *egzamin na ocenę – pisemny lub ustny*

C. Podstawowe kryteria
- *uzyskanie pozytywnej oceny*

Określenie przedmiotów wprowadzających wraz z wymogami wstępnymi
Należy określić:
A. Wymagania formalne:
B. Wymagania wstępne:

Cele przedmiotu
Przedmiot stanowi przegląd algebraicznych metod kryptografii

Treści programowe

A. Problematyka wykładu
1 Podzielność w pierścieniu liczb całkowitych, liczby pierwsze, algorytm Euklidesa.
2 Relacja przystawania modulo, twierdzenie Gaussa, twierdzenie Fermata, funkcja Eulera.
3 Arytmetyka ciał pierwotnych Zp i ich struktura algebraiczna.
4 Teoria podzielności w pierścieniach wielomianów, reprezentacja ciał skończonych jako pierścieni ilorazowych i struktura algebraiczna ciał p^n elementowych.
5 Logarytm dyskretny i algorytmy jego obliczania.
6 Przegląd historyczny systemów kryptograficznych od starożytności do XIX wieku.

7	Proste systemy algebraiczne wykorzystujące pojęcia i własności ciał Zp.
8	Systemy kryptograficzne wykorzystujące pojęcia algebry liniowej, macierze szyfrujące.
9	Pojęcie kryptograficznego klucza publicznego, symetryczne i asymetryczne systemy kryptograficzne.
10	Opis i działanie systemu RSA.
11	System ElGamala podpisu cyfrowego, zastosowanie logarytmu dyskretnego.
12	Elementy analizy kryptograficznej, analiza różnicowa i liniowa.
13	Elementy teorii krzywych eliptycznych .
14	Systemy kryptograficzne wykorzystujące pojęcie krzywych eliptycznych.
15	Przegląd współczesnych trendów w stosowaniu pojęć algebraicznych do kryptografii.

Wykaz literatury

A. Literatura wymagana

A.1. **wykorzystywana podczas zajęć**/A.2. **studiowana samodzielnie przez studenta**

1. J.A. Buchmann. Wprowadzenie do kryptografii.
2. N.Koblitz, Wykład z teorii liczb i kryptografii.
3. N.Koblitz, Algebraiczne aspekty kryptografii.
4. B. Schreier. Kryptografia dla praktyków.

Efekty kształcenia

Wiedza

Symb.	Efekt	Metoda weryfikacji	Odniesienie
W01	Znajomość podstaw kryptografii	sprawdzian pisemny	K_W04,05

Umiejętności:

Symb.	Efekt	Metoda weryfikacji	Odniesienie
U01	Stosuje wybrane metody kryptografii	sprawdzian pisemny, sprawdzian z wykorzystaniem pakietu matematycznego	K_U04,14

Kompetencje społeczne (postawy)

Symb.	Efekt	Metoda weryfikacji	Odniesienie
K01	zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia	konwersacja	K_K01
K02	potrafi precyzyjnie formułować pytania, zarówno werbalnie w trakcie zajęć jak i na potrzeby agregatów wyszukujących i naukowych baz danych, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania		K_K02,06

Kontakt:

Wykaz numerów telefonicznych i adresów mailowych pracowników znajduje się na stronie Instytutu Matematyki i Informatyki: `www.math.uni.opole.pl`