UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Kryptografia z elementami algebry

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka **Specjalność** - **Jednostka organizacyjna** Wydział Matematyki i Informatyki **Poziom studiów** studia inżynierskie pierwszego stopnia **Forma studiów** studia niestacjonarne **Profil studiów** profil ogólnoakademicki	**Cykl dydaktyczny** 2024/25 **Kod zajęć** 06INFN.38P.04805.24 **Języki wykładowe** polski **Obligatoryjność** Obowiązkowy **Blok zajęciowy** Przedmioty podstawowe

Koordynator zajęć	Maciej Grześkowiak
Prowadzący zajęcia	Maciej Grześkowiak

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 4	• Wykład: 15, Egzamin • Ćwiczenia: 8, Zaliczenie z oceną • Ćwiczenia w salach komputerowych: 12, Zaliczenie z oceną	5

Cele kształcenia dla zajęć

Kod	Cel
C1	Prezentacja podstawowych algorytmów i protokołów kryptologicznych.
C2	Pokazanie struktur algebraicznych wykorzystywanych w kryptografii.
C3	Kształtowanie umiejętności implementacji struktur algebraicznych.
C4	Rozwój umiejętności programistycznych studenta.
C5	Kształtowanie umiejętności wykorzystania aparatu matematycznego w procesie analizy i systemu informatycznego.
C6	Kształtowanie umiejętności poprawnego użycia popularnych implementacji algorytmów i protokołów kryptograficznych.

Wymagania wstępne

1. Znajomość metod programowania
2. Znajomość elementarnej teorii liczb
3. Znajomość podstawowych struktur algebraicznych

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Zna strukturę algebraiczną związaną z systemem kryptograficznym.	INF_K3_W01, INF_K3_W02	Egzamin pisemny, Kolokwium pisemne, Projekt
W2	Zna współczesną terminologię kryptologiczną.	INF_K3_W01, INF_K3_W02, INF_K3_W03	Egzamin pisemny
Umiejętności – Student/ka:			
U1	Potrafi zaimplementować działania na elementach struktur algebraicznych.	INF_K3_U01_inz, INF_K3_U05_inz, INF_K3_U07_inz	Projekt
U2	Wykorzystuje twierdzenia matematyczne w analizie systemów kryptograficznych.	INF_K3_U01_inz, INF_K3_U02	Egzamin pisemny, Kolokwium pisemne
U3	Analizuje bezpieczeństwo algorytmów kryptologicznych. Potrafi wskazać wady i zalety danego rozwiązania kryptologicznego.	INF_K3_U04_inz, INF_K3_U06_inz	Egzamin pisemny
U4	Potrafi obliczyć złożoność obliczeniową algorytmów wykorzystywanych do konstrukcji systemów kryptologicznych.	INF_K3_U01_inz, INF_K3_U06_inz	Egzamin pisemny, Kolokwium pisemne

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Działania wewnętrzne w zbiorze i ich własności. Zasadnicze pojęcia teorii grup – podgrupy, warstwy.	W1, U1	Wykład, Ćwiczenia
2.	Operacje elementarne na bitach. Notacja wielkie O. Algorytmy czasu wielomianowego oraz wykładniczego ze względu na liczbę bitów danych.	W2, U4	Wykład, Ćwiczenia
3.	Podstawowe protokoły kryptograficzne. Bezpieczeństwo doskonałe. Bezpieczeństwo obliczeniowe. Kandydaci na funkcje jednokierunkowe. Problem logarytmu dyskretnego w grupie. Problem i-tego bitu logarytmu dyskretnego.	W2, U2, U3	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
4.	Rząd elementu w grupie. Grupy cykliczne. Homomorfizm grup. Jądro oraz obraz homomorfizmu. Grupa ilorazowa i twierdzenie o izomorfizmie.	W1, U2	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
5.	Algorytmy szyfrowania z kluczem publicznym. Algorytm ElGamala i RSA. Obliczanie logarytmu dyskretnego metodą wielkich i małych kroków. Równoważność między problemem faktoryzacji a łamaniem RSA.	W1, U1, U3	Wykład, Ćwiczenia
6.	Użycie klucza publicznego na przykładzie GPG. Generowanie, przedłużanie i wygaszanie kluczy. Szyfrowanie, podpisywanie, weryfikacja plików i maili. Budowanie łańcucha zaufania – podpisywanie kluczy.	W2	Ćwiczenia w salach komputerowych
7.	Ciała skończone i ich własności. Reszty i niereszty kwadratowe w grupach skończonych. Obliczanie pierwiastków w ciałach skończonych.	W1, U1	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
8.	Krzywe eliptyczne nad ciałem skończonym. Generowanie krzywej eliptycznej. Kodowanie wiadomości na krzywej. Algorytm obliczanie n-tej wielokrotności punktu krzywej eliptycznej.	W1, W2, U1, U2	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
9.	Algorytm ElGamala na krzywej eliptycznej. Problem logarytmu dyskretnego na krzywej eliptycznej. Protokoły uzgadniania kluczy. Protokół Diffiego-Hellmana na krzywej eliptycznej. Wykorzystanie ECDH na przykładzie openvpn.	W1, W2, U1, U3	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
10.	Symetryczny protokół szyfrowania. Standard szyfrowania danych DES i jego modyfikacje. Tryby pracy szyfrów blokowych.	W1, W2, U3	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
11.	Pierścienie. Jedności pierścieni. Obraz i jądro homomorfizmu pierścieni. Pierścienie wielomianów. Algorytm Euklidesa dla wielomianów. Ideały i pierścienie ilorazowe.	W1, W2, U1, U2	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
12.	Zaawansowany standard szyfrowania danych AES. Tranformacje SubByte i MixColumn w AES Użycie AES do szyfrowania plików i dysków na przykładzie cryptsetup.	W1, W2, U1, U2, U3	Wykład, Ćwiczenia, Ćwiczenia w salach komputerowych
13.	Funkcje hashujące. Atak urodzinowy. Gdzie występują, czym się charakteryzują, użycie ich we własnym kodzie.	U1, U3, U4	Wykład, Ćwiczenia w salach komputerowych
14.	Uwierzytelnienie. Poufność, wiarygodność i zaufanie: w przeglądarce internetowej. SSL/TLS na przykładzie openssl w budowaniu VPN, na przykładzie openvpn.	W2, U3	Wykład, Ćwiczenia w salach komputerowych

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny
Ćwiczenia	Metoda ćwiczeniowa, Metoda badawcza (dociekania naukowego)
Ćwiczenia w salach komputerowych	Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Egzamin połówkowy 0-50pkt Egzamin połówkowy podczas sesji egzaminacyjnej 0-50pkt Ocena z egzaminu, to suma punktów z dwóch egzaminów połówkowych: 50pkt - 59pkt 3.0 60pkt-69pkt 3.5 70pkt-79pkt 4.0 80pkt-89pkt 4.5 90pkt-100pkt 5.0
Ćwiczenia	Kolokwium I 0-50-pkt Kolokwium II 0-50-pkt Ocena z ćwiczeń, to suma punktów z dwóch kolokwów: 50pkt - 59pkt 3.0 60pkt-69pkt 3.5 70pkt-79pkt 4.0 80pkt-89pkt 4.5 90pkt-100pkt 5.0
Ćwiczenia w salach komputerowych	Na ocenę z ćwiczeń w salach komputerowych składają się 4 projekty, punktowane 0-50 pkt każdy. Ocena jest zależna od sumy punktów z projektów: 100pkt - 119pkt 3.0 120pkt-139pkt 3.5 140pkt-159pkt 4.0 160pkt-179pkt 4.5 180pkt-200pkt 5.0

Literatura

Obowiązkowa

1. Mirosław Kutyłowski, Willy-B. Strothmann, ,,Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych'', Wydawnictwo READ ME, 1998
2. Neal Koblitz, ,,Wykład z teorii liczb i kryptografii'', Wydawnictwa Naukowo-Techniczne, 1994.
3. Jerzy Rutkowski, Algebra abstrakcyjna w zadaniach, Wydawnictwo Naukowe PWN, 2005.

Dodatkowa

1. Jerzy Browkin, Wybrane zagadnienia z algebry, Wydawnictwo Naukowe PWN, 1968.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Wykład	15
Ćwiczenia	8
Ćwiczenia w salach komputerowych	12
Przygotowanie projektu	25
Przygotowanie do zaliczenia	20
Przygotowanie do zajęć	20
Przygotowanie do egzaminu	25
Łączny nakład pracy studenta	**Liczba godzin** 125
Liczba punktów ECTS	**ECTS** 5

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K3_U01_inz	Absolwent/ka potrafi zastosować wiedzę matematyczną do formułowania, modelowania, analizowania i rozwiązywania prostych zadań związanych z informatyką
INF_K3_U02	Absolwent/ka potrafi pozyskiwać wiarygodne informacje z literatury, baz wiedzy, Internetu oraz innych źródeł, integrować je, interpretować oraz wyciągać wnioski i formułować opinie
INF_K3_U04_inz	Absolwent/ka potrafi opracować, przeanalizować, zaprojektować klasyczne algorytmy i systemy informatyczne
INF_K3_U05_inz	Absolwent/ka potrafi pisać, uruchamiać i testować programy w wybranym środowisku programistycznym
INF_K3_U06_inz	Absolwent/ka potrafi ocenić, na podstawowym poziomie, przydatność metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do typowych zadań informatycznych
INF_K3_U07_inz	Absolwent/ka potrafi zastosować wybrane metody wykorzystywane w wiodących kierunkach badań informatyki
INF_K3_W01	Absolwent/ka zna i rozumie zaawansowane pojęcia z działów matematyki służące do modelowania i rozwiązywania problemów w informatyce
INF_K3_W02	Absolwent/ka zna i rozumie zaawansowane pojęcia i problemy formujące kanon dyscypliny informatyka
INF_K3_W03	Absolwent/ka zna i rozumie narzędzia, technologie i urządzenia informatyczne właściwe dla wybranych obszarów zastosowań oraz podstawy ich działania