UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Kryptografia

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka **Specjalność** - **Jednostka organizacyjna** Wydział Matematyki i Informatyki **Poziom studiów** studia drugiego stopnia poinżynierskie **Forma studiów** studia stacjonarne **Profil studiów** profil ogólnoakademicki	**Cykl dydaktyczny** 2023/24 **Kod zajęć** 06INFS.41S.00997.23 **Języki wykładowe** polski **Obligatoryjność** Fakultatywny **Blok zajęciowy** Przedmioty specjalnościowe

Koordynator zajęć	Maciej Grześkowiak
Prowadzący zajęcia	Maciej Grześkowiak

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 1	• Wykład: 15, Zaliczenie z oceną • Ćwiczenia: 7, Zaliczenie z oceną • Laboratorium: 8, Zaliczenie z oceną	3

Cele kształcenia dla zajęć

Kod	Cel
C1	Prezentacja współczesnych algorytmów i protokołów kryptograficznych.
C2	Poznanie charakterystyki bezpiecznego systemu informatycznego.
C3	Rozwój umiejętności programistycznych studenta.
C4	Nabycie umiejętności analizowania bezpieczeństwa systemu informatycznego.
C5	Nabycie umiejętności wykorzystania aparatu matematycznego w procesie analizy i tworzenia systemu informatycznego.

Wymagania wstępne

Umiejętność programowania na poziomie inżyniera informatyki. Znajomość elementów algebry i teorii liczb.

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 i rozumie współczesne podstawowe protokoły kryptograficzne i metody szyfrowania danych.	INF_K4_W01, INF_K4_W03, INF_K4_W04	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć
W2	zna i rozumie zagadnienia związane z integralnością i uwierzytelnianiem danych.	INF_K4_W01, INF_K4_W03, INF_K4_W04	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć
Umiejętności – Student/ka:			
U1	potrafi korzystać z klasycznych protokołów kryptograficznych w komunikacji danych.	INF_K4_U01, INF_K4_U11	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć
U2	potrafi szyfrować, sprawdzać integralność i uwierzytelniać dane przy pomocy metod kryptograficznych.	INF_K4_U01, INF_K4_U03, INF_K4_U11	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć
Kompetencji społecznych – Student/ka:			
K1	rozumie konsekwencje stosowania technik kleptograficznych.	INF_K4_K06	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Podstawowe protokoły kryptograficzne. Symetryczny protokół szyfrowania. Doskonały schemat szyfrowania.	U1	Wykład, Ćwiczenia, Laboratorium
2.	Bezpieczeństwo obliczeniowe. EAV-secure schemat szyfrowania. Pseudolosowość.	W1, U1	Wykład, Ćwiczenia, Laboratorium
3.	Ataki z wybranym tekstem jawnym. CPA-secure schemat szyfrowania. Szyfrowanie strumieniowe.	W1, U1	Wykład, Ćwiczenia, Laboratorium
4.	Integralność i uwierzytelnianie danych. Message Authentication Codes. CCA-secure schemat szyfrowania.	W2, U2	Wykład, Ćwiczenia, Laboratorium
5.	Szyfrowanie uwierzytelnione. Funkcje hashujące. HMAC.	W1, W2, U1, U2	Wykład, Ćwiczenia, Laboratorium
6.	Grupy skończone. Problemy obliczeniowe w grupach skończonych. Protokoły uzgadniania klucza sesyjnego.	W1, U1	Wykład, Ćwiczenia, Laboratorium
7.	EAV, CPA oraz CCA bezpieczny schemat szyfrowania z kluczem publicznym.	W1, U1	Wykład, Ćwiczenia, Laboratorium
8.	Szyfrowanie hybrydowe oraz KEM/DEM.	W1, U1	Wykład, Ćwiczenia, Laboratorium
9.	Podpisy cyfrowe.	W2, U2	Wykład, Ćwiczenia, Laboratorium
10.	Kanały podprogowe.	W1, U1	Wykład, Ćwiczenia, Laboratorium
11.	Techniki kleptograficzne.	K1	Wykład, Ćwiczenia, Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień
Ćwiczenia	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda ćwiczeniowa
Laboratorium	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda laboratoryjna, Metoda projektu, Praca w grupach

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem przystąpienia do kolokwium pisemnego jest uzyskanie zaliczenia z ćwiczeń i laboratoriów. Na końcową ocenę składa się wynik uzyskany na kolokwium pisemnym. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Forma zajęć	Warunki zaliczenia zajęć
Ćwiczenia	Na końcową ocenę składa się wynik uzyskany z kolokwium pisemnego. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Laboratorium	Końcowa ocena składa się z następujących elementów: 1. projekt – 50%, 2. zadania wykonywane podczas zajęć – 50%. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

1. Jonathan Katz, Yehuda Lindell, "Introduction to modern cryptography", Taylor & Francis Inc., 2014.
2. Neal Koblitz, "Wykład z teorii liczb i kryptografii", Wydawnictwa Naukowo-Techniczne, 1994.
3. William Stallings, "Cryptography and Network Security", Pearson Education, Inc, 2006.
4. Mirosław Kutyłowski, Willy-B. Strothmann, "Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych", Wydawnictwo READ ME, 1998.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15
Ćwiczenia	7
Laboratorium	8
Przygotowanie do zajęć	10
Czytanie wskazanej literatury	10
Przygotowanie projektu	15
Przygotowanie do zaliczenia	10
Łączny nakład pracy studenta	**Liczba godzin** 75
Liczba punktów ECTS	**ECTS** 3

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_K06	Absolwent/ka jest gotów/gotowa do pogłębiania świadomości roli informatyki w kształtowaniu życia społecznego
INF_K4_U01	Absolwent/ka potrafi zastosować zaawansowaną wiedzę matematyczną do formułowania, analizowania i rozwiązywania złożonych i nietypowych zadań związanych z informatyką
INF_K4_U03	Absolwent/ka potrafi stosować zaawansowane metody budowy oprogramowania, rozstrzyga o ich przydatności, w tym podejmuje decyzje dotyczące wyboru technik prowadzących do otrzymania oprogramowania wysokiej jakości
INF_K4_U11	Absolwent/ka potrafi pozyskiwać informacje z literatury, baz wiedzy, Internetu oraz innych wiarygodnych źródeł, integrować je, dokonywać ich interpretacji oraz wyciągać wnioski i formułować opinie
INF_K4_W01	Absolwent/ka zna i rozumie w pogłębionym stopniu pojęcia z działów matematyki niezbędne do rozwiązywania zaawansowanych problemów w informatyce
INF_K4_W03	Absolwent/ka zna i rozumie w pogłębionym stopniu współczesne metody, narzędzia i technologie informatyczne właściwe dla wybranych obszarów zastosowań niezbędne przy budowie złożonych systemów informatycznych oraz przy prowadzeniu prac badawczo-rozwojowych
INF_K4_W04	Absolwent/ka zna i rozumie zasady rozwiązywania problemów z wykorzystaniem zaawansowanych algorytmów i metod informatycznych