AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nazwa modułu zajęć: Matematyczne podstawy kryptologii

Rok akademicki: 2019/2020 Kod: ZSDA-3-0260-s Punkty ECTS: 4

Wydział: Szkoła Doktorska AGH

Kierunek: Szkoła Doktorska AGH Specjalność: —

Poziom studiów: Studia III stopnia Forma studiów: Stacjonarne

Język wykładowy: Polski Profil: Ogólnoakademicki (A) Semestr: 0

Strona www: —

Prowadzący moduł: dr hab. Foryś Wit (foryswit@wms.mat.agh.edu.pl)

Treści programowe zapewniające uzyskanie efektów uczenia się dla modułu zajęć

wykład prezentuje aktualne krypto-systemy i protokoły ze szczególnym naciskiem na ich matematyczne podstawy (teorię liczb, ciał skończonych, krzywych eliptycznych) i teorię złożoności obliczeniowej.

Opis efektów uczenia się dla modułu zajęć

Kod MEU	Student, który zaliczył moduł zajęć zna i rozumie/potrafi/jest gotów do	Powiązania z KEU	Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć
Wiedza: zna i rozumie			
M_W001	zna podstawowe pojęcia, zasady i metody kryptografii i kryptoanalizy	SDA3A_W02	Egzamin
M_W002	zna podstawowe pojęcia, własnosci, i algorytmy teorii liczb	SDA3A_W02	Egzamin
M_W003	zna podstawowe pojęcia, własności i algorytmy kryptografii klucza publicznego	SDA3A_W01	Egzamin
M_W004	zna podstawowe pojęcia, własności i protokoły wykorzystujące kryptografię klucza publicznego	SDA3A_W02, SDA3A_W01	Egzamin
Umiejętności: potrafi			
M_U001	potrafi implementować poznane algorytmy i protokołu	SDA3A_U03, SDA3A_U02, SDA3A_U01	Egzamin

Kompetencje społeczne: jest gotów do			
M_K001	potrafi wykorzystać wyszukana przez siebie literaturę specjalistyczną	SDA3A_K01, SDA3A_K02	Egzamin

Liczba godzin zajęć w ramach poszczególnych form zajęć

	Forma zajęć dydaktycznych										
Suma	Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Prace kontrolne i przejściowe	Lektorat
30	30	0	0	0	0	0	0	0	0	0	0

Matryca kierunkowych efektów uczenia się w odniesieniu do form zajęć i sposobu zaliczenia, które pozwalają na ich uzyskanie

Kod MEU	Student, który zaliczył moduł zajęć zna i rozumie/potrafi/jest gotów do	Forma zajęć dydaktycznych										
		Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Prace kontrolne i przejściowe	Lektorat
Wiedza: zna i rozumie												
M_W001	zna podstawowe pojęcia, zasady i metody kryptografii i kryptoanalizy	+	-	-	-	-	-	-	-	-	-	-
M_W002	zna podstawowe pojęcia, własnosci, i algorytmy teorii liczb	+	-	-	-	-	-	-	-	-	-	-
M_W003	zna podstawowe pojęcia, własności i algorytmy kryptografii klucza publicznego	+	-	-	-	-	-	-	-	-	-	-
M_W004	zna podstawowe pojęcia, własności i protokoły wykorzystujące kryptografię klucza publicznego	+	-	-	-	-	-	-	-	-	-	-
Umiejętności: potrafi												
M_U001	potrafi implementować poznane algorytmy i protokołu	+	-	-	-	-	-	-	-	-	-	-
Kompetencje społeczne: jest gotów do												
M_K001	potrafi wykorzystać wyszukana przez siebie literaturę specjalistyczną	+	-	-	-	-	-	-	-	-	-	-

Nakład pracy studenta (bilans punktów ECTS)

Forma aktywności studenta	Obciążenie studenta
Udział w zajęciach dydaktycznych/praktyka	30 godz
Przygotowanie do zajęć	20 godz
przygotowanie projektu, prezentacji, pracy pisemnej, sprawozdania	10 godz
Samodzielne studiowanie tematyki zajęć	2 godz
Egzamin lub kolokwium zaliczeniowe	20 godz
Sumaryczne obciążenie pracą studenta	82 godz
Punkty ECTS za moduł	4 ECTS

Pozostałe informacje

Szczegółowe treści kształcenia w ramach poszczególnych form zajęć (szczegółowy program wykładów i pozostałych zajęć)

Wykład

matematyczne podstawy kryptologii klasycznej
Klasyczne (symetryczne) kryptosystemy monoalfabetyczne i polialfabetyczne (kryptosystem Cezara, Hilla, afiniczny, Vigenere'a,
Beauforta, Playfaira);
twierdzenia i algorytmy z arytmetyki modularnej i podstaw teorii liczb

matematyczne podstawy kryptosystemów nowoczesnych I
DES, schemat Feistela; kryptoanaliza różnicowa; metody probabilistyczne (3 godz.)
AES; elementy ciał Galois
Idea klucza publicznego, funkcje jednokierunkowe ; problem plecakowy i kryptosystem plecakowy
Algorytm Shamira przełamania kryptosystemu plecakowego, elementy teorii krat i algorytm LLL; tw. uzasadniajace poprawność

matematyczne podstawy kryptosystemów nowoczesnych II
RSA
Liczby pseudopierwsze – testy pierwszości: Fermata, Solovaya-Strassena, Millera-Rabina;
Problemy faktoryzacji; algorytm oparty na krzywych eliptycznych; podstawy teorii krzywych eliptycznych
Logarytm dyskretny i przydzielanie kluczy; ciała Galois cd. ; kryptosystem Rabina, ElGamala, McEliece; podpis elektroniczny -
wykorzystanie RSA

krzywe eliptyczne w kryptografii
Krzywe eliptyczne; kryptografia na krzywych eliptycznych część I
Krzywe eliptyczne; kryptografia na krzywych eliptycznych część II

Protokoły kryptograficzne
Protokół kryptograficzny – wprowadzenie; Rzut monetą przez telefon; poker telefoniczny

Częściowe odkrywanie sekretu; Dowody o wiedzy zerowej

Metody i techniki kształcenia:
Wykład: wykład z wykorzystaniem technik multimedialnych i programu MATHEMATICA

Warunki i sposób zaliczenia poszczególnych form zajęć, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:
egzamin – egzamin ustny lub przygotowanie projektu pisemnego (do wyboru). Wszyscy dopuszczeni do egzaminu.

Zasady udziału w poszczególnych zajęciach, ze wskazaniem, czy obecność studenta na zajęciach jest obowiązkowa:
Wykład:
– Obecność obowiązkowa: Tak
– Zasady udziału w zajęciach: aktywna obecność

Sposób obliczania oceny końcowej
na podstawie oceny z egzaminu

Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach:
kontakt bezpośredni – konsultacje lub kontakt meilowy

Wymagania wstępne i dodatkowe, z uwzględnieniem sekwencyjności modułów
ukończone studia I i II stopnia

Zalecana literatura i pomoce naukowe
1] N.Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa, 1995
[2] R.A.Mollin, RSA and Public-Key Cryptography, Chapman_Hall CRC, 2003
[3] B. Schneier, Applied cryptography, John Wiley&Sons, 1994
[3] W.Trappe, L.C.Washington, Introduction to cryptography with Coding Theory,
Prentice Hall, 2002
[4] L.C.Washington, Elliptic Curves, Number Theory and Cryptography, Chapman_Hall CRC, 2003
[5] Internet – strony www wskazane na wykładzie

Publikacje naukowe osób prowadzących zajęcia związane z tematyką modułu
W.Foryś, Ł.Jęda, P.Oprocha, On a Cipher Based on Pseudo-random Walks on Graphs, Communications in Computer and Information Science 448, 2014 pp.59-73

Informacje dodatkowe
Brak