AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nazwa modułu zajęć: Kryptografia ()

Rok akademicki: 2019/2020 Kod: AMAT-2-013-MU-s Punkty ECTS: 4

Wydział: Matematyki Stosowanej

Kierunek: Matematyka Specjalność: Matematyka ubezpieczeniowa

Poziom studiów: Studia II stopnia Forma studiów: Stacjonarne

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

Strona www: —

Prowadzący moduł: dr hab. Foryś Wit (wforys@agh.edu.pl)

Treści programowe zapewniające uzyskanie efektów uczenia się dla modułu zajęć

Podstawowe pojęcia, zasady i metody kryptografii i kryptoanalizy.

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, własnosci, i algorytmy teorii liczb	MAT2A_W11, MAT2A_W01, MAT2A_K05, MAT2A_W07	Odpowiedź ustna, Kolokwium, Egzamin, Aktywność na zajęciach
M_W002	Potrafi projektować i implementować podstawowe kryptosystemy	MAT2A_U01, MAT2A_U02, MAT2A_K05	Odpowiedź ustna, Kolokwium, Egzamin, Aktywność na zajęciach
M_W003	zna podstawowe pojęcia, zasady i metody kryptografii i kryptoanalizy	MAT2A_W11, MAT2A_W01, MAT2A_W02, MAT2A_W04, MAT2A_U13, MAT2A_U02, MAT2A_W05	Odpowiedź ustna, Kolokwium, Egzamin, Aktywność na zajęciach
Umiejętności: potrafi			
M_U001	zna podstawowe pojęcia, własności i protokoły wykorzystujące kryptografię klucza publicznego	MAT2A_U20, MAT2A_U21, MAT2A_U14, MAT2A_U01, MAT2A_U02, MAT2A_U03	Odpowiedź ustna, Kolokwium, Egzamin, Aktywność na zajęciach

M_U002	Potrafi projektować i implementować podstawowe kryptosystemy klucza publicznego	MAT2A_U01, MAT2A_W02, MAT2A_K02, MAT2A_U02, MAT2A_U03, MAT2A_K01	Odpowiedź ustna, Kolokwium, Egzamin, Aktywność na zajęciach
M_U003	zna podstawowe pojęcia, własności i algorytmy kryptografii klucza publicznego	MAT2A_U19, MAT2A_U21, MAT2A_W04, MAT2A_U13, MAT2A_W07, MAT2A_U03	Odpowiedź ustna, Kolokwium, Egzamin, Aktywność na zajęciach
Kompetencje społeczne: jest gotów do			
M_K001	umie ocenić stopień zrozumienia przez siebie problemu i brakujące elementy rozumowania	MAT2A_K07, MAT2A_K02, MAT2A_K01	Odpowiedź ustna, Kolokwium, Egzamin, Aktywność na zajęciach

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
60	30	30	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, własnosci, i algorytmy teorii liczb	+	+	-	-	-	-	-	-	-	-	-
M_W002	Potrafi projektować i implementować podstawowe kryptosystemy	+	+	-	-	-	-	-	-	-	-	-
M_W003	zna podstawowe pojęcia, zasady i metody kryptografii i kryptoanalizy	+	+	-	-	-	-	-	-	-	-	-
Umiejętności: potrafi												

M_U001	zna podstawowe pojęcia, własności i protokoły wykorzystujące kryptografię klucza publicznego	+	+	-	-	-	-	-	-	-	-	-
M_U002	Potrafi projektować i implementować podstawowe kryptosystemy klucza publicznego	+	+	-	-	-	-	-	-	-	-	-
M_U003	zna podstawowe pojęcia, własności i algorytmy kryptografii klucza publicznego	+	+	-	-	-	-	-	-	-	-	-
Kompetencje społeczne: jest gotów do												
M_K001	umie ocenić stopień zrozumienia przez siebie problemu i brakujące elementy rozumowania	+	+	-	-	-	-	-	-	-	-	-

Nakład pracy studenta (bilans punktów ECTS)

Forma aktywności studenta	Obciążenie studenta
Udział w zajęciach dydaktycznych/praktyka	60 godz
Samodzielne studiowanie tematyki zajęć	33 godz
Egzamin lub kolokwium zaliczeniowe	2 godz
Dodatkowe godziny kontaktowe	5 godz
Sumaryczne obciążenie pracą studenta	100 godz
Punkty ECTS za moduł	4 ECTS

Pozostałe informacje

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

Wykład

1. Twierdzenia i algorytmy z arytmetyki modularnej i podstaw teorii liczb

2. Klasyczne (symetryczne) kryptosystemy monoalfabetyczne i polialfabetyczne (kryptosystem Cezara,
Hilla, afiniczny, Vigenere’a, Beaufort’a, Playfair’a)

3. Maszyny rotorowe – ENIGMA; podstawy teoretyczne; historia; tw. ktore rozstrzygnęło II wojnę światową

4. DES, schemat Feistela; kryptoanaliza rożnicowa; metody probabilistyczne
AES; elementy ciał Galois

5. Idea klucza publicznego, funkcje jednokierunkowe ; problem plecakowy i

kryptosystem plecakowy

6. Algorytm Shamira przełamania kryptosystemu plecakowego, elementy teorii krat i algorytm LLL

7. RSA

8. Liczby pseudopierwsze – testy pierwszości: Fermata, Solovaya-Strassena, Millera-Rabina

9. Podpis elektroniczny –
Logarytm dyskretny i przydzielanie kluczy; ciała Galois cd. ; kryptosystem Rabina, ElGamala, McEliece;

10. Protokoł kryptograficzny – wprowadzenie; Rzut monetą przez telefon; poker telefoniczny

11. Częściowe odkrywanie sekretu;

12. Dowody o wiedzy zerowej

13. Krzywe eliptyczne; kryptografia na krzywych eliptycznych

14. Problemy faktoryzacji; algorytm oparty na krzywych eliptycznych; podstawy teorii krzywych eliptycznych

Ćwiczenia audytoryjne

Program ćwiczeń pokrywa się z programem wykładu
Rozwiązywanie (głównie algorytmiczne) problemów ilustrujących treści przekazywane na wykładach.

Metody i techniki kształcenia:

Wykład: Treści prezentowane na wykładzie są przekazywane w formie prezentacji multimedialnej w połączeniu z klasycznym wykładem tablicowym wzbogaconymi o pokazy odnoszące się do prezentowanych zagadnień.
Ćwiczenia audytoryjne: Podczas zajęć audytoryjnych studenci na tablicy rozwiązują zadane wcześniej problemy. Prowadzący na bieżąco dokonuje stosowanych wyjaśnień i moderuje dyskusję z grupą nad danym problemem.

Warunki i sposób zaliczenia poszczególnych form zajęć, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:

Nie określono

Zasady udziału w poszczególnych zajęciach, ze wskazaniem, czy obecność studenta na zajęciach jest obowiązkowa:

Wykład:
– Obecność obowiązkowa: Tak
– Zasady udziału w zajęciach: Studenci uczestniczą w zajęciach poznając kolejne treści nauczania zgodnie z syllabusem przedmiotu. Studenci winni na bieżąco zadawać pytania i wyjaśniać wątpliwości. Rejestracja audiowizualna wykładu wymaga zgody prowadzącego.
Ćwiczenia audytoryjne:
– Obecność obowiązkowa: Tak

– Zasady udziału w zajęciach: Studenci przystępując do ćwiczeń są zobowiązani do przygotowania się w zakresie wskazanym każdorazowo przez prowadzącego (np. w formie zestawów zadań). Ocena pracy studenta może bazować na wypowiedziach ustnych lub pisemnych w formie kolokwium, co zgodnie z regulaminem studiów AGH przekłada się na ocenę końcową z tej formy zajęć.

Sposób obliczania oceny końcowej
zaliczenie

Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach:
Student powinien zgłosić się do prowadzącego w celu ustalenia indywidualnego sposobu nadrobienia zaległości.

Wymagania wstępne i dodatkowe, z uwzględnieniem sekwencyjności modułów
Nie podano wymagań wstępnych lub dodatkowych.

Zalecana literatura i pomoce naukowe
Moduł ma charakter autorski, obowiązuje przede wszystkim materiał wyłożony, literatura ma charakter pomocniczy. Literatura podana jest na początku wykładu i wskazywana na bieżąco w trakcie wykładu.

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
4. W.Trappe, L.C.Washington, *Introduction to cryptography with Coding Theory*, Prentice Hall, 2002
5. L.C.Washington, *Elliptic Curves, Number Theory and Cryptography_, Chapman*Hall CRC, 2003
6. Internet – strony www wskazane na wykładzie

Publikacje naukowe osób prowadzących zajęcia związane z tematyką modułu
1. Foryś, Wit; Matyja, Janusz; On one-sided, topologically mixing cellular automata, having continuum of fixed points and topological entropy log(n) for any integer n>1; J. Cell. Autom. 9, No. 1, 37-58 (2014).

2. Foryś, Wit; Matyja, Janusz; On one-sided, D-chaotic cellular automaton, having continuum of fixed points and topological entropy log(3); J. Cell. Autom. 8, No. 3-4, 131-146 (2013).

3. Foryś, Wit; Matyja, Janusz; On one-sided, D-chaotic cellular automata, having continuum of fixed points and topological entropy log(p) for any prime p>3; J. Cell. Autom. 7, No. 4, 303-319 (2012).

4. Foryś, Wit; Oprocha, Piotr; Infinite traces and symbolic dynamics – the minimal shift case; Fundam. Inform. 111, No. 2, 147-161 (2011).

Informacje dodatkowe
Brak