Państwowa Wyższa Szkoła Zawodowa w Nowym Sączu

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2012/2013

Instytut Techniczny

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: Stacjonarne

Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

PWSZ w Nowym Sączu

1 Przedmiot

Nazwa przedmiotu	Kryptografia i teoria kodów
Kod przedmiotu	IT 11.3 AIS C12 12/13
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	1
Semestry	7

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	wykład	ćwiczenia	laboratorium	projekt	seminarium
7	15				

3 Cele przedmiotu

Cel 1 Zapoznanie studenta z elementami algebraicznej teorii kodowania.

Cel 2 Zdobycie przez studenta wiedzy z zakresu operacji modularnych.

Cel 3 Obeznanie studenta ze strukturami algebraicznymi: pierścienie, ciała i grupy.

Cel 4 Nabycie przez studenta wiedzy o charakterystykach, typach, strukturze i zdolności detekcyjnej i korekcyjnej kodów korekcyjnych.

Cel 5 Zaznajomienie studenta z binarnymi kodami blokowymi liniowymi i cyklicznymi.

©M. Aleksander, I. Borczuch, S. Świgut

Cel 6 Pozyskanie przez studenta wiedzy w zakresie systemów kryptograficznych.

Cel 7 Zapoznanie studenta z kryptografią klucza publicznego.

Cel 8 Uzyskanie przez studenta wiedzy z zakresu technik kryptografii symetrycznej.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

a Matematyka dyskretna.

b Metody probabilistyczne i statystyka.

c Podstawy programowania.

d Języki i paradygmaty programowania.

5 Efekty kształcenia

EK1 Wiedza: Student opisuje i zaprezentuje elementy algebraicznej teorii kodowania.

EK2 Wiedza: Student powiązuje, wybiera i argumentuje operacje modularne i w ciałach skończonych.

EK3 Wiedza: Student objaśnia struktury algebraiczne: pierścienie, ciała i grupy.

EK4 Wiedza: Student definiuje, wyjaśnia i porównuje charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych.

EK5 Wiedza: Student uogólnia, używa i porównuje binarne kody blokowe liniowe i cykliczne.

EK6 Wiedza: Student objaśnia działanie systemów kryptograficznych.

EK7 Wiedza: Student powie, zaklasyfikuje, interpretuje i uzasadnia kryptografię klucza publicznego.

EK8 Wiedza: Student rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej.

6 Treści programowe

PWSZ w Nowym Sączu

wykład

Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Elementy algebraicznej teorii kodowania. Arytmetyka modularna.	2
W2	Struktury algebraiczne: pierścienie, ciała i grupy.	2
W3	Charakterystyka, typy, struktura oraz zdolność detekcyjna i korekcyjna kodów korekcyjnych, metody kodowego zabezpieczenia przed błędami w transmisji.	2
W4	Binarne kody blokowe liniowe i cykliczne, kody Hamminga, generacja kodów, realizacja techniczna. Kody uwierzytelniania.	2
W5	Klasyczne systemy kryptograficzne.	1
W6	Kryptografia klucza publicznego.	2
W7	Kryptografia symetryczna.	4
	Razem	**15**

7 Metody dydaktyczne

M1 Wykłady

©M. Aleksander, I. Borczuch, S. Świgut

M2 Prezentacje multimedialne

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	15
Konsultacje przedmiotowe	1
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	5
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	4
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**25**
Sumaryczna liczba punktów ECTS dla przedmiotu	1

9 Sposoby oceny

Po zakończeniu wykładu przeprowadza się dyskusja kierowana na omawiany temat. Prowadzący ocenia odpowiedzi udzielone przez studentów na postawione pytania.

Ocena formująca

F1 Aktywność na zajęciach

F2 Odpowiedź ustna

Ocena podsumowująca

P1 Referat

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 3	Student nazywa i opisuje podstawowe elementy algebraicznej teorii kodowania, ale z błędami.
Na ocenę 4	Student zna motywacje badań nad algebraiczną teorią kodowania i potrafi poprawnie wymienić oraz krótko scharakteryzować podstawowe elementy algebraicznej teorii kodowania.
Na ocenę 5	Student doskonale opisuje oraz ze znawstwem i bezbłędnie prezentuje wszystkie zawarte na wykładzie elementy algebraicznej teorii kodowania.
Efekt kształcenia 2	
Na ocenę 3	Student nazywa i powiązuje wybrane operacje modularne i w ciałach skończonych, ale z błędami.
Na ocenę 4	Student powiązuje, wybiera i argumentuje podstawowe operacje modularne i w ciałach skończonych, z drobnymi nieścisłościami.
Na ocenę 5	Student objaśnia ze znawstwem operacje modularne i w ciałach skończonych, podając i charakteryzując przykłady.
Efekt kształcenia 3	
Na ocenę 3	Student definiuje pojęcia struktur algebraicznych: pierścieni, ciał i grup, ale z błędami.

PWSZ w Nowym Sączu

©M. Aleksander, I. Borczuch, S. Świgut

Na ocenę 4	Student prawidłowo objaśnia struktury algebraiczne: pierścienie, ciała i grupy.
Na ocenę 5	Student doskonale objaśnia struktury algebraiczne, posługując się definicjami pierścieni, ciał i grup oraz potrafi wskazać i scharakteryzować przykłady.
Efekt kształcenia 4	
Na ocenę 3	Student definiuje i wyjaśnia wybrane charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych.
Na ocenę 4	Student definiuje, wyjaśnia i porównuje podstawowe charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych, z drobnymi nieścisłościami.
Na ocenę 5	Student doskonale definiuje, wyjaśnia i porównuje podstawowe charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych. Podaje i charakteryzuje przykłady.
Efekt kształcenia 5	
Na ocenę 3	Student uogólnia i porównuje binarne kody blokowe liniowe i cykliczne, ale z błędami.
Na ocenę 4	Student uogólnia i porównuje binarne kody blokowe liniowe i cykliczne, ale z błędami, z drobnymi nieścisłościami.
Na ocenę 5	Student doskonale uogólnia i porównuje ze znawstwem binarne kody blokowe liniowe i cykliczne oraz potrafi ich użyć.
Efekt kształcenia 6	
Na ocenę 3	Student definiuje pojęcie systemu kryptograficznego, ale z błędami. Wymienia tylko niektóre elementy systemu kryptograficznego.
Na ocenę 4	Student prawidłowo definiuje pojęcie systemu kryptograficznego i objaśnia poprawnie jego działanie.
Na ocenę 5	Student definiuje ze znawstwem pojęcie systemu kryptograficznego i doskonale objaśnia jego działanie, posługując się pojęciami technicznymi, oraz potrafi wskazać zastosowanie systemu kryptograficznego.
Efekt kształcenia 7	
Na ocenę 3	Student podaje definicję i określa podstawowe cechy kryptografii klucza publicznego, ale z błędami.
Na ocenę 4	Student zna, klasyfikuje, interpretuje i uzasadnia kryptografię klucza publicznego, z drobnymi nieścisłościami.
Na ocenę 5	Student powie ze znawstwem o kryptografii klucza publicznego, podaje jej klasyfikację, doskonale uzasadniając i interpretując jej zastosowanie.
Efekt kształcenia 8	
Na ocenę 3	Student nazywa i rozpoznaje techniki kryptografii symetrycznej, ale z błędami.
Na ocenę 4	Student rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej, z drobnymi nieścisłościami.
Na ocenę 5	Student doskonale rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej. Podaje przykłady.

PWSZ w Nowym Sączu

10 Macierz realizacji przedmiotu

Efekty kształcenia dla przedmiotu	Odniesienie do efektów kierunkowych	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Sposoby oceny
EK1	INF_W01	Cel1	W1	M1, M2	F1, F2, P1
EK2	INF_W01, INF_W16	Cel2	W1	M1, M2	F1, F2, P1
EK3	INF_W01, INF_W16	Cel3	W2	M1, M2	F1, F2, P1
EK4	INF_W01	Cel4	W3	M1, M2	F1, F2, P1

©M. Aleksander, I. Borczuch, S. Świgut

Efekty kształcenia dla przedmiotu	Odniesienie do efektów kierunkowych	Cele przedmiotu	Treści programowe	Metody dydaktyczne	Sposoby oceny
EK5	INF_W01	Cel5	W4	M1, M2	F1, F2, P1
EK6	INF_W16	Cel6	W5	M1, M2	F1, F2, P1
EK7	INF_W16	Cel7	W6	M1, M2	F1, F2, P1
EK8	INF_W16	Cel8	W7	M1, M2	F1, F2, P1

11 Wykaz literatury

Literatura podstawowa:

[1] Foryś W., Foryś M. — *Teoria języków formalnych i automatów*, Warszawa, 2005, AOW EXIT

[2] Karbowski M. — *Podstawy kryptografii. Wydanie II*, Gliwice, 2007, HELION

[3] Karpiński M. — *Bezpieczeństwo informacji*, Warszawa, 2012, PAK

[4] Mochnacki W. — *Kody korekcyjne i kryptografia*, Wrocław, 2000, Oficyna Wydawnicza

[5] Stinson D.R. — *Kryptografia w teorii i w praktyce*, Warszawa, 2004, WNT

Literatura uzupełniająca:

[1] Blake I., Seroussi G., Smart N. — *Krzywe eliptyczne w kryptografii*, Warszawa, 2004, WNT

[2] Bauer F. L. — *Sekrety kryptografii. Metody i zasady kryptografii*, Gliwice, 2003, HELION

[3] Koblitz N. — *Wykład z teorii liczb i kryptografii*, Warszawa, 2006, WNT

[4] Kościelny C., Kurkowski M., Srebrny M. — *Kryptografia - teoretyczne podstawy i praktyczne*, Warszawa, 2009, Polsko-Japońska Wyższa Szkoła Technik Komputerowych

[5] Welschenbach M. — *Kryptografia w C i C++*, Warszawa, 2002, MIKOM

[6] Karpiński M., Kurytnik I.P. — *Sieci komputerowe: Bezpieczeństwo. Część 1 Metody i systemy kryptograficzne*, Bielsko-Biała, 2006, ATH

PWSZ w Nowym Sączu

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

mgr Grzegorz Litawa (kontakt: glitawa@poczta.onet.pl)

Osoby prowadzące przedmiot

prof. dr hab. inż. Mikołaj Karpiński (kontakt: mkarpinski@ath.bielsko.pl)

dr hab. Wit Foryś (kontakt: forysw@mail.ii.uj.edu.pl)

dr inż. Ihor Pazdriy (kontakt: irpazdriy@gmail.com)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (kierownik zakładu) (dyrektor instytutu)

 licencja bezpłatna dla PWSZ w Nowym Sączu
©M. Aleksander, I. Borczuch, S. Świgut

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

.....

.....

.....

PWSZ w Nowym Sączu

©M. Aleksander, I. Borczuch, S. Świgut