

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: Niestacjonarne

Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

1 PRZEDMIOT

NAZWA PRZEDMIOTU	Kryptografia i teoria kodów
KOD PRZEDMIOTU	IT 11.3 AIN 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	8				

3 CELE PRZEDMIOTU

Cel 1 Zapoznanie studenta z elementami algebraicznej teorii kodowania.

Cel 2 Zdobywanie 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.



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

WYKŁAD

LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Elementy algebraicznej teorii kodowania. Arytmetyka modularna.	1
W2	Struktury algebraiczne: pierścienie, ciała i grupy.	1
W3	Charakterystyka, typy, struktura oraz zdolność detekcyjna i korekcyjna kodów korekcyjnych, metody kodowego zabezpieczenia przed błędami w transmisji.	1
W4	Binarne kody blokowe liniowe i cykliczne, kody Hamminga, generacja kodów, realizacja techniczna. Kody uwierzytelniania.	1
W5	Klasyczne systemy kryptograficzne.	1
W6	Kryptografia klucza publicznego.	1
W7	Kryptografia symetryczna.	2
	RAZEM	8

7 METODY DYDAKTYCZNE

M1 Wykłady



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	8
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	10
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	6
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.



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.

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



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

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

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



PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....
.....
.....

PWSZ w Nowym Sączu