Państwowa Wyższa Szkoła Zawodowa w Nowym Sączu

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2016/2017

Instytut Techniczny

Kierunek studiów: Informatyka | Profil: Praktyczny

Forma studiów: Stacjonarne | Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

1 Przedmiot

Nazwa przedmiotu	Kryptografia i teoria kodów
Kod przedmiotu	IT 11.3 PIS C14 16/17
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	2
Semestry	7

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	wykład	ćwiczenia	laboratorium	projekt	seminarium
7				30	

3 Cele przedmiotu

Cel 1 Zapoznanie studenta z elementami algebraicznej teorii kodowania,operacji modularnych,strukturami algebraicznymi.

Cel 2 Nabycie przez studenta wiedzy o charakterystykach, typach, strukturze i zdolności detekcyjnej i korekcyjnej kodów korekcyjnych oraz kodach binarnych.

Cel 3 Pozyskanie przez studenta wiedzy w zakresie systemów i technik kryptograficznych.

Cel 4 Zapoznanie studenta z kryptografią klucza publicznego.

Cel 5 Nabycie umiejętności określania przydatności i doboru odpowiednich technik kryptograficznych.

Cel 6 Nabycie umiejętności implementacji określonych technik kryptograficznych w budowanych systemach.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

a Metody probabilistyczne i statystyka.

b Podstawy programowania.

5 Efekty kształcenia

EK1 Wiedza: Student opisuje i objaśnia elementy algebraicznej teorii kodowania, operacje modularne w ciałach skończonych, struktury algebraiczne.

EK2 Wiedza: Student definiuje, wyjaśnia i porównuje charakterystyki, typy, struktury binarnych kodów blokowych liniowych i cyklicznych oraz zdolności detekcyjne i korekcyjne kodów korekcyjnych.

EK3 Wiedza: Student objaśnia działanie systemów kryptograficznych, rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej.

EK4 Wiedza: Student klasyfikuje, interpretuje i uzasadnia kryptografie klucza publicznego.

EK5 Umiejętności: Student posiada umiejętności określania przydatności i doboru odpowiednich technik kryptograficznych.

EK6 Umiejętności: Student potrafi dokonać implementacji określonych technik kryptograficznych w budowanych systemach.

6 Treści programowe

PROJEKT

Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Projekt systemu kryptograficznego klucza publicznego.	6
P2	Projekt systemu kryptograficznego na podstawie algorytmow symetrycznych.	6
P3	Projekt systemu bezpieczeństwa IT w oparaciu o metody kryptograficzne.	6
P4	Projekt bezpiecznego systemu przekazu informacji oparty o systemy kryptograficzne bazujące na krzywych eliptycznych.	6
P5	Projekt uwzględniający aspekty - do wyboru: 1. Elementy algebraicznej teorii kodowania Arytmetykę modularna, 2. Struktury algebraiczne: pierścienie, ciała i grupy. 3. Charakterystykę, typy, strukturę oraz zdolność detekcyjna i korekcyjna kodów korekcyjnych, metody kodowego zabezpieczenia przed błędami w transmisji. 4. Binarne kody blokowe liniowe i cykliczne, kody Haimninga, generację kodów, realizację techniczną. Kody uwierzytelniania.	6
	Razem	**30**

7 Metody dydaktyczne

M1 Ćwiczenia projektowe

M2 Projekty

M3 Praca w grupach

M4 Dyskusja

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	30
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	4
Opracowanie wyników	5
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**50**
Sumaryczna liczba punktów ECTS dla przedmiotu	2

9 Sposoby oceny

Ocena formująca

F1 Projekt indywidualny

F2 Projekt zespołowy

F3 Odpowiedź ustna

Ocena aktywności bez udziału nauczyciela akademickiego

1 Projekt zespołowy

Kryteria oceny

Efekt kształcenia 1		Miejsce weryfikacji	Opis weryfikacji EK 1
Na ocenę 3	Student nazywa i opisuje podstawowe elementy algebraicznej teorii kodowania, wybrane operacje modularne i w ciałach skończonych, struktur algebraicznych, ale popełnia błędy .	projekt	Ocena z odpowiedzi ustnych i projektów.
Na ocenę 4	Student zna motywacje badań nad algebraiczną teorią kodowania i potrafi poprawnie wymienić oraz krótko scharakteryzować podstawowe elementy algebraicznej teorii kodowania, struktury algebraiczne, ma problemy z argumentacją operacji modularnych w ciałach skończonych.		
Na ocenę 5	Student opisuje bezbłędnie elementy algebraicznej teorii kodowania, objaśnia ze zrozumieniem operacje modularne i w ciałach skończonych, struktur algebraicznych, podając i charakteryzując przykłady.		

Efekt kształcenia 2		Miejsce weryfikacji	Opis weryfikacji EK 2
Na ocenę 3	Student definiuje i wyjaśnia wybrane charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych, uogólnia i porównuje binarne kody blokowe liniowe i cykliczne, ale z błędami.	projekt	Ocena z odpowiedzi ustnych i projektów.
Na ocenę 4	Student definiuje, wyjaśnia i porównuje podstawowe charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych, z drobnymi nieścisłościami. Uogólnia i porównuje binarne kody blokowe liniowe i cykliczne z drobnymi nieścisłościami.		
Na ocenę 5	Student doskonale definiuje, wyjaśnia i porównuje podstawowe charakterystyki, typy, struktury i zdolności detekcyjne i korekcyjne kodów korekcyjnych. Uogólnia i porównuje ze zrozumieniem binarne kody blokowe, liniowe i cykliczne oraz potrafi ich użyć. Podaje i charakteryzuje przykłady.		
Efekt kształcenia 3		Miejsce weryfikacji	Opis weryfikacji EK 3
Na ocenę 3	Student definiuje pojęcie systemu kryptograficznego nazywa i rozpoznaje najważniejsze techniki kryptografii symetrycznej. Wymienia tylko niektóre elementy systemu kryptograficznego.	projekt	Ocena z odpowiedzi ustnych i projektów.
Na ocenę 4	Student prawidłowo definiuje pojęcie systemu kryptograficznego i objaśnia poprawnie jego działanie, rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej, z drobnymi nieścisłościami.		
Na ocenę 5	Student definiuje ze zrozumieniem pojęcie systemu kryptograficznego i doskonale objaśnia jego działanie, posługując się pojęciami technicznymi, oraz potrafi wskazać zastosowanie systemu kryptograficznego. Rozpoznaje, kategoryzuje i ocenia techniki kryptografii symetrycznej. Podaje przykłady.		
Efekt kształcenia 4		Miejsce weryfikacji	Opis weryfikacji EK 4
Na ocenę 3	Student podaje definicję i określa podstawowe cechy kryptografii klucza publicznego, ale z błędami.	projekt	Ocena z odpowiedzi ustnych i projektów.
Na ocenę 4	Student zna, klasyfikuje, interpretuje i uzasadnia stosowanie kryptografii klucza publicznego, z drobnymi nieścisłośsciami.		
Na ocenę 5	Student zna i rozumieniem zasady kryptografii klucza publicznego, podaje jej klasyfikację, doskonale uzasadniając i interpretując jej zastosowanie.		

Efekt kształcenia 5		Miejsce weryfikacji	Opis weryfikacji EK 5
Na ocenę 3	Student posiada umiejętności określania przydatności odpowiednich technik kryptograficznych, Student posiada umiejętności określania przydatności i doboru odpowiednich technik kryptograficznych, zna wymagania stawiane systemom kryptograficznym, ma problemy z doborem odpowiednich techniki do rozwiązywanych problemów.	projekt	Ocena z odpowiedzi ustnych i projektów.
Na ocenę 4	Student posiada umiejętności określania przydatności i doboru odpowiednich technik kryptograficznych do rozwiązywanych problemów.		
Na ocenę 5	Student posiada umiejętności określania przydatności i doboru odpowiednich technik kryptograficznych, zna wymagania stawiane systemom kryptograficznym potrafi dobrać odpowiednie techniki do rozwiązywanych problemów.		
Efekt kształcenia 6		Miejsce weryfikacji	Opis weryfikacji EK 6
Na ocenę 3	Student potrafi dokonać implementacji podstawowych technik kryptograficznych w budowanych systemach.	projekt	Ocena z odpowiedzi ustnych i projektów.
Na ocenę 4	Student potrafi dokonać implementacji zaawansowanych technik kryptograficznych w budowanych systemach.		
Na ocenę 5	Student dokonuje implementacji zaawansowanych technik kryptograficznych w budowanych systemach, potrafi stosować niestandardowe rozwiązania w budowanych systemach.		

Ocena do indeksu (ocena podsumowująca)

Średnia ważona ocen cząstkowych uzyskanych za poszczególne efekty kształcenia.

Warunki zaliczenia przedmiotu

a Pozytywna ocena wykonanych projektów i ustnej odpowiedzi.

10 Macierz realizacji przedmiotu

Efekty kształcenia dla przedmiotu	Odniesienie do efektów kierunkowych	Cele przedmiotu	Treści programowe	Metody dydaktyczne
EK1	INFP_W01	Cel1	P2, P5	M2, M4

Efekty kształcenia dla przedmiotu	Odniesienie do efektów kierunkowych	Cele przedmiotu	Treści programowe	Metody dydaktyczne
EK2	INFP_W01, INFP_W08	Cel2	P3, P5	M2, M4
EK3	INFP_W01, INFP_W08	Cel3	P1, P2, P3, P4	M2, M4
EK4	INFP_UP05, INFP_W08	Cel4	P1, P4	M2, M4
EK5	INFP_UP05, INFP_W01	Cel5	P1, P3	M2, M4
EK6	INFP_UP05, INFP_W08	Cel5, Cel6	P1, P2, P3, P4	M1, M3, M4

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

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

Literatura uzupełniająca:

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

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

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

[4] Koscielny C., Kurkowski M., Srebrny M. — *Kryptografia - teoretyczne podstawy i praktyczne*, Warszawa, 2009, Polsko-Japońska Wyzsza Szko la Technik Komputerowych

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

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

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

Osoby prowadzące przedmiot

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

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

.....