

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: Niestacjonarne

Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

1 PRZEDMIOT

NAZWA PRZEDMIOTU	Kryptografia i teoria kodów
KOD PRZEDMIOTU	IT 11.3 PIN 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				15	

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.	3
P2	Projekt systemu kryptograficznego na podstawie algorytmów symetrycznych.	3
P3	Projekt systemu bezpieczeństwa IT w oparciu o metody kryptograficzne.	3
P4	Projekt bezpiecznego systemu przekazu informacji oparty o systemy kryptograficzne bazujące na krzywych eliptycznych.	3
P5	Projekt uwzględniający aspekty - do wyboru: 1. Elementy algebraicznej teorii kodowania Arytmetykę modularną, 2. Struktury algebraiczne: pierścienie, ciała i grupy. 3. Charakterystykę, typy, strukturę oraz zdolność detekcyjną i korekcyjną kodów korekcyjnych, metody kodowego zabezpieczenia przed błędami w transmisji. 4. Binarne kody blokowe liniowe i cykliczne, kody Hamminga, generację kodów, realizację techniczną. Kody uwierzytelniania.	3
	RAZEM	15

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	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	10
Opracowanie wyników	5
Przygotowanie raportu, projektu, prezentacji, dyskusji	19
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 modułowe 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 modułowych w ciałach skończonych.		
NA OCENĘ 5	Student opisuje bezbłędnie elementy algebraicznej teorii kodowania, objaśnia ze zrozumieniem operacje modułowe 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 nieścisłościami.		
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 doбором 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. — *Wykład z teorii liczb i kryptografii*, Warszawa, 2006, WNT
- [4] Koscielny 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

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)

.....

PWSZ w Nowym Sączu