

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla inżynierów

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Zaawansowane techniki kryptografii i kryptoanalizy
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Advanced cryptography and cryptanalysis
KOD PRZEDMIOTU	WiIT I oIIS D7 19/20
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	7.00
SEMESTRY	2

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
2	30	30	15	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Nauczenie studentów wybranych metod współczesnej kryptologii.

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1 Podstawy algebry i teorii liczb

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Student zna wybrane algorytmy szyfrujące i ich podstawy matematyczne

EK2 Umiejętności Student potrafi zastosować wybrane algorytmy szyfrujące

EK3 Wiedza Student zna wybrane metody podpisu cyfrowego i ich podstawy matematyczne

EK4 Wiedza Student potrafi zastosować wybrane algorytmy podpisu cyfrowego

6 TREŚCI PROGRAMOWE

LABORATORIUM		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
L1	Kryptografia klasyczna	3
L2	Szyfry symetryczne i bezpieczeństwo informacji	3
L3	Szyfry asymetryczne	3
L4	Szyfry strumieniowe	3
L5	Podpisy cyfrowe	3

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Teoria liczb i podstawy kryptologii	4
C2	Kryptografia klasyczna: Proste szyfry podstawieniowe. Szyfry homofoniczne. Szyfry podstawieniowe wieloalfabetowe. Szyfry poligramowe. Szyfry przestawieniowe, szyfry afiniczne. Bezpieczne systemy kryptograficzne (konfuzja, dyfuzja, kompromisy, kryptoanaliza).	6
C3	Prawdopodobieństwo i tajność doskonała. Teoria Shannona: Entropia. Problem plecakowy, problem faktoryzacji, problem pakowania, problemy NP-zupełne.	4
C4	Szyfry symetryczne i bezpieczeństwo informacji: Szyfry Feistela. Kryptografia i bezpieczeństwo informacji. Algorytm DES/AES.	5
C5	Szyfry asymetryczne: Szyfrowanie z kluczem publicznym. Bezpieczeństwo. RSA. Szyfr Rabina, szyfr ElGamala.	5

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C6	Szyfry strumieniowe	3
C7	Podpisy cyfrowe: Standard podpisu cyfrowego (DSS). Dzielenie sekretu.	3

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Wybrane zagadnienia teorii liczb	4
W2	Elementy kryptologii: Ochrona danych. Systemy i algorytmy kryptograficzne. Własności informacyjne języka.	2
W3	Kryptografia klasyczna: Proste szyfry podstawieniowe. Szyfry homofoniczne. Szyfry podstawieniowe wieloalfabetowe. Szyfry poligramowe. Szyfry przestawieniowe, szyfry afiniczne. Bezpieczne systemy kryptograficzne (konfuzja, dyfuzja, kompromisy, kryptoanaliza).	6
W4	Prawdopodobieństwo i tajność doskonała. Teoria Shannona: Entropia. Problem plecakowy, problem faktoryzacji, problem pakowania, problemy NP-zupełne.	4
W5	Szyfry symetryczne i bezpieczeństwo informacji: Szyfry Feistela. Kryptografia i bezpieczeństwo informacji. Algorytm DES/AES.	4
W6	Szyfry asymetryczne: Szyfrowanie z kluczem publicznym. Bezpieczeństwo. RSA. Szyfr Rabina, szyfr ElGamala.	4
W7	Szyfry strumieniowe	3
W8	Podpisy cyfrowe: Standard podpisu cyfrowego (DSS). Dzielenie sekretu.	3

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady

N2 Zadania tablicowe

N3 Ćwiczenia laboratoryjne

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	75
Konsultacje przedmiotowe	5
Egzaminy i zaliczenia w sesji	5
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	85
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	40
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	210
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	7.00

9 SPOSOBY OCENY

OCENA PODSUMOWUJĄCA

P1 Egzamin pisemny

P2 Egzamin ustny

P3 Ocena z ćwiczeń

P4 Ocena z laboratorium

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Warunkiem otrzymanie oceny pozytywnej z ćwiczeń jest uczestnictwo w zajęciach, aktywność na zajęciach, uzyskanie przynajmniej 50% z możliwych do zdobycia punktów.

W2 Warunkiem otrzymanie oceny pozytywnej z laboratorium jest uczestnictwo w zajęciach, aktywność na zajęciach, uzyskanie przynajmniej 50% z możliwych do zdobycia punktów.

W3 Do egzaminu mogą przystąpić jedynie studenci, którzy otrzymali ocenę pozytywną z ćwiczeń i laboratorium.

W4 Na ocenę końcową z przedmiotu ma wpływ ocena P1, P2, P3 i P4.

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie spełnił wymagań na ocenę 3.0.

NA OCENĘ 3.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 50%.
NA OCENĘ 3.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 60%.
NA OCENĘ 4.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 70%.
NA OCENĘ 4.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 80%.
NA OCENĘ 5.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 90%.
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie spełnił wymagań na ocenę 3.0.
NA OCENĘ 3.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 50%.
NA OCENĘ 3.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 60%.
NA OCENĘ 4.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 70%.
NA OCENĘ 4.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 80%.
NA OCENĘ 5.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 90%.
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie spełnił wymagań na ocenę 3.0.
NA OCENĘ 3.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 50%.
NA OCENĘ 3.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 60%.
NA OCENĘ 4.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 70%.
NA OCENĘ 4.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 80%.
NA OCENĘ 5.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 90%.
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie spełnił wymagań na ocenę 3.0.

NA OCENĘ 3.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 50%.
NA OCENĘ 3.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 60%.
NA OCENĘ 4.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 70%.
NA OCENĘ 4.5	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 80%.
NA OCENĘ 5.0	Student ma wiedzę z przedstawionego na zajęciach materiału na poziomie przynajmniej 90%.

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1	I2_W01 I2_W02	Cel 1	L1 L2 L3 L4 C1 C2 C3 C4 C5 C6 W1 W2 W3 W4 W5 W6	N1 N2 N3	P1 P2 P3 P4
EK2	I2_W01 I2_W02 I2_U07 I2_U08	Cel 1	L1 L2 L3 L4 C1 C2 C3 C4 C5 C6 W1 W2 W3 W4 W5 W6 W7	N1 N2 N3	P1 P2 P3 P4
EK3	I2_W01 I2_W02	Cel 1	L1 L2 L3 L4 L5 C1 C2 C3 C4 C5 C6 C7 W1 W2 W3 W4 W5 W6 W7 W8	N1 N2 N3	P1 P2 P3 P4
EK4	I2_W01 I2_W02 I2_U07 I2_U08	Cel 1	L1 L2 L3 L4 L5 C1 C2 C3 C4 C5 C6 C7 W1 W2 W3 W4 W5 W6 W7 W8	N1 N2 N3	P1 P2 P3 P4

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | D. R. Stinson — *Kryptografia (w teorii i w praktyce)*, Warszawa, 2005, WNT
- [2] | 9.N. Ferguson, B. Schneider — *Practical Cryptography*, , 2003, Wiley Publ. Inc.,
- [3] | N. Koblitz — *Algebraiczne aspekty kryptografii*, Warszawa, 2000, WNT
- [4] | J. Gancarzewicz — *Arytmetyka*, Kraków, 2002, Wydawnictwo UJ

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr Grzegorz Gancarzewicz (kontakt: grzegorz.gancarzewicz@pk.edu.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)