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 sudiów: stacjonarne | Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla licencjatów

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	3

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
3	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

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

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
C1	Teoria liczb i podstawy kryptologii	4

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
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
C6	Szyfry strumieniowe	3
C7	Podpisy cyfrowe: Standard podpisu cyfrowego (DSS). Dzielenie sekretu.	3

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

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	W1 W2 W3 W4 W5 W6 C1 C2 C3 C4 C5 C6 L1 L2 L3 L4	N1 N2 N3	P1 P2 P3 P4
EK2	I2_U12	Cel 1	W1 W2 W3 W4 W5 W6 W7 C1 C2 C3 C4 C5 C6 L1 L2 L3 L4	N1 N2 N3	P1 P2 P3 P4
EK3	I2_W01 I2_W02	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 C1 C2 C3 C4 C5 C6 C7 L1 L2 L3 L4 L5	N1 N2 N3	P1 P2 P3 P4
EK4	I2_W01 I2_U07 I2_U12	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 C1 C2 C3 C4 C5 C6 C7 L1 L2 L3 L4 L5	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: gancarz@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)