KARTA PRZEDMIOTU DLA NABORU 2020/2021

INFORMACJE OGÓLNE

1. **Nazwa przedmiotu kształcenia**

KRYPTOGRAFIA

2. **Nazwa jednostki prowadzącej moduł** Wydział Nauk Technicznych, Zakład Informatyki
3. **Grupa treści kształcenia** -
4. **Typ przedmiotu** obowiązkowy
5. **Poziom studiów** pierwszego stopnia
6. **Liczba punktów ECTS** 3
7. **Poziom przedmiotu** podstawowy
8. **Rok studiów, semestr** II rok, semestr 4
9. **Liczba godzin w semestrze** wykład 15, laboratorium 30
10. **Język wykładowy:** polski
11. **Wykładowca (wykładowcy)**

INFORMACJE SZCZEGÓŁOWE

12. Wymagania wstępne

1. Znajomość podstaw matematyki (teoria liczb, (mnożenie i odwracanie macierzy, eliminacja Gaussa))
2. Znajomość podstaw z zakresu informatyki (znajomość podstaw programowania)

13. Cele przedmiotu

C1 zapoznanie studentów z zadaniami i narzędziami kryptografii

C2 Zaznajomienie z podstawowymi metodami szyfrów klasycznych i wprowadzenie do metod nowoczesnych.

C3 Przekazanie studentom wiedzy z zakresu kryptograficznych metod ochrony danych i praktycznego ich zastosowania

14. Efekty uczeniasięw zakresie wiedzy, umiejętności i kompetencji społecznych

Student, który zaliczył przedmiot potrafi:	odniesienie do kierunkowych efektów uczenia się
WIEDZA	
EU01 Zna i rozumie podstawowe pojęcia kryptografii i kryptoanalizy.	I1P_W04 I1P_W05 I1P_W26
EU02 Dysponuje wiedzą na temat teoretycznych podstaw kryptografii: teorii informacji, teorii złożoności obliczeniowej i teorii liczba.	
EU03 Zna narzędzia i protokoły, wykorzystujące w sposób praktyczny algorytmy kryptograficzne.	
UMIEJĘTNOŚCI	
EU04 potrafi użyć technik kryptograficznych do zabezpieczenia komunikacji	I1P_U01 I1P_U07 I1P_U29
EU05 potrafi szyfrować i deszyfrować z użyciem określonego systemu kryptograficznego	
EU06 Potrafi stosować podstawowe techniki zabezpieczenia danych	
KOMPETENCJE SPOŁECZNE	
EU16 Potrafi odpowiedzialnie rozwiązywać zadania problemowe w grupie.	I1P_K04

15. Treści programowe

Forma zajęć – wykłady

W1. Wprowadzenie do kryptografii. Podstawowe pojęcia i definicja bezpieczeństwa systemu informatycznego oraz kryteria systemów, techniczne środki utrzymania bezpieczeństwa.

W2. Historia i rozwój kryptografii i kryptoanalizy. Historyczne systemy kryptograficzne. Sposoby utajniania informacji w przeszłości. Współczesny stan metod kryptograficznych.

W3. Klasyfikacja i omówienie ataków na systemy kryptograficzne. Polityka bezpieczeństwa systemów kryptograficznych.

W4. Kryptografia a teoria kodowania Systemy kryptograficzne. Szyfrowanie danych symetryczne i asymetryczne.
W5. Klasyczne systemy kryptograficzne Kryptografia a steganografia. Szyfry cykliczne i antycykliczne. Permutacje alfabetu i szyfry transpozycyjne.
W6. Metody uwierzytelniania - protokoły PAP, CHAP, EAP, protokoły wykorzystujące poznane mechanizmy kryptograficzne - symetryczne, asymetryczne i funkcje skrótu
W7. Kryptografia współczesna System RSA. Logarytm dyskretny i kryptosystemy na nim oparte

Forma zajęć –laboratoria

L1. Szyfry klasyczne i ich łamanie, analiza częstości występowania liter.
L2. Implementacja generatora ciągów losowych BBS, oraz 4 podstawowych testów sprawdzających losowość wygenerowanego ciągu.
L3. Implementacja wybranego trybu pracy szyfrów blokowych, przy wykorzystaniu podstawowego trybu pracy ECB, ocena propagacji błędów w różnych trybach pracy
L4. Szyfry n-dzielne, kwadraty szyfrujące
L5. Macierze szyfrujące
L6. RSA i algorytmy rozkładu liczb na czynniki- zastosowanie
L7. Podpis elektroniczny
L8. Enigma – budowa i działanie
L9. Konfiguracja bezpiecznej autoryzacji z wykorzystaniem protokołu Kerberos
L10. Powtórzenie / zaliczenie końcowe

16. Narzędzia/metody dydaktyczne

1. Prezentacja multimedialna.
2. Podstawowe narzędzia informatyczne – komputer i oprogramowanie

17. Sposoby oceny (F – formująca; P – podsumowująca)

F1.	Ocena bieżącego przygotowania do zajęć laboratoryjnych
F2.	Sprawozdanie z laboratorium
P1.	Kolokwium
P2.	Ocena pracy na zajęciach
P2.	Zaliczenie końcowe - egzamin

18. Obciążenia pracą studenta

forma aktywności	średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem*	45+10
Nakład pracy studenta	
Przygotowanie się do zajęć	5
Przygotowanie ćwiczeń/laboratoriów	5
Przygotowanie projektu	10
SUMA	75
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3

19. Literatura podstawowa i uzupełniająca

Literatura podstawowa:

1. Stokłosa J. (red.), Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo Politechniki Poznańskiej, Poznań,
2. Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion
3. Kryptografia. W teorii i praktyce, Douglas R. Stinson, WNT.
4. Kryptografia dla praktyków, Bruce Schneier, WNT.
5. Kryptografia stosowana, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, WNT

Literatura uzupełniająca:

1. Teoria liczb w praktyce, Song Y. Yan, PWN, 2006.
2. Łamacze kodów. Historia kryptologii, David Kahn, WNT 2004.

20. Formy oceny - szczegóły

Warunki uzyskania zaliczenia przedmiotu: zajęcia kończą się egzaminem.

Sposób weryfikacji efektów uczenia się:

Ocena stopnia osiągniętych przez studenta efektów uczenia się następuje wg poniższych kryteriów:
5.0 – zakładany efekt uczenia się został osiągnięty bez zastrzeżeń
4.5 – zakładany efekt uczenia się został osiągnięty z pojedynczymi brakami/błędami
4.0 – zakładany efekt uczenia się został osiągnięty z nielicznymi brakami/błędami
3.5 – zakładany efekt uczenia się został osiągnięty z wieloma brakami/błędami
3.0 – zakładany efekt kształcenia został osiągnięty z licznymi i istotnymi brakami/błędami (minimalnie wymagany poziom osiągnięcia efektu)
2.0 – zakładany efekt uczenia się nie został osiągnięty

21. Inne przydatne informacje o przedmiocie

1. Bezpośrednich informacji o problematyce zajęć i treściach programowych udziela Prowadzący w trakcie zajęć i podczas konsultacji
2. Zajęcia odbywać się będą w PSW w Białej Podlaskiej
3. Zajęcia odbywać się będą zgodnie z aktualnym planem zajęć
4. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem

* Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innej osoby prowadzącej zajęcia oraz konsultacje