WYDZIAŁ INFORMATYKI I ZARZĄDZANIA

KARTA PRZEDMIOTU

Nazwa w języku polskim Kryptografia
Nazwa w języku angielskim Cryptography
Kierunek studiów (jeśli dotyczy): Informatyka
Specjalność (jeśli dotyczy): Bezpieczeństwo i Niezawodność Systemów Informatycznych
Stopień studiów i forma: II stopień, niestacjonarna
Rodzaj przedmiotu: obowiązkowy
Kod przedmiotu INZ4187
Grupa kursów NIE

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	18		18		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	120		90		
Forma zaliczenia	Egzamin		Zaliczenie na ocenę		
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	4		3		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0		3		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	1,6		1,2		

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1. Podstawowa znajomość analizy matematycznej, algebry oraz rachunku prawdopodobieństwa i statystyki.
2. Umiejętność programowania w języku wyższego poziomu (Java, C++, C#, Python).

\

CELE PRZEDMIOTU

C1 Nabycie podstawowej wiedzy w zakresie podstaw matematycznych kryptografii.
C2 Nabycie podstawowej wiedzy o algorytmach kryptograficznych.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy student:

PEK_W01 – zna podstawy matematyczne dotyczące funkcjonowania algorytmów kryptograficznych,

PEK_W02 – posiada wiedzę z zakresu funkcjonowania algorytmów kryptograficznych.

Z zakresu umiejętności student:

PEK_U01 – potrafi zaimplementować proste algorytmy kryptograficzne w języku programowania wysokiego poziomu,

PEK_U02 – ma przygotowanie niezbędne do pracy w pracowniach komputerowych i zna zasady bezpieczeństwa związane z tą pracą.

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Wprowadzenie do kursu. Kryptologia, kryptografia, kryptoanaliza – definicje, terminologia. Historia kryptografii i kryptoanalizy.	1
Wy2	Podstawy matematyczne – wybrane zagadnienia z teorii informacji, teorii liczb i złożoności obliczeniowej.	1
Wy3	Systemy kryptograficzne, ich elementy składowe oraz właściwości.	1
Wy4	Kroki szyfrowania - Podstawienia i transpozycje.	1
Wy5	Szyfrowanie polialfebetyczne.	1
Wy6	Szyfry blokowe i strumieniowe.	2
Wy7	Algorytmy kryptograficzne z kluczem symetrycznym.	2
Wy8	Algorytmy kryptograficzne z kluczem publicznym.	2
Wy9	Generatory ciągów losowych – generowanie kluczy.	1
Wy10	Generowanie liczb pierwszych. Jednokierunkowe funkcje skrótu.	1
Wy11	Podpisy cyfrowe. Certyfikaty i infrastruktura klucza publicznego.	1
Wy12	Protokoły kryptograficzne	1
Wy13	Systemy kryptograficzne na krzywych eliptycznych i hipereliptycznych.	1
Wy14	Kryptoanaliza i metody kryptoanalityczne - wybrane zagadnienia (cz.1)	1
Wy15	Kryptoanaliza i metody kryptoanalityczne - wybrane zagadnienia (cz.2)	1
	Suma godzin	**18**

Forma zajęć - laboratorium		**Liczba godzin**
La1	Zajęcia organizacyjne. Szkolenie BHP.	1
La2	Zapoznanie z dostępnym oprogramowaniem edukacyjnym z dziedziny kryptografii i kryptoanalizy.	1
La3	Pakiety matematyczne do obliczeń kryptograficznych.	1

La4	Implementacja szkieletu aplikacji sieciowej do nauki technik i algorytmów kryptograficznych.	1
La5	Implementacja prostych algorytmów kryptograficznych (Alg. Cezara, itp.).	1
La6	Implementacja bardziej zaawansowanych algorytmów kryptograficznych (Alg Viginere'a).	1
La7	Techniki monitorowania ruchu sieciowego w celu weryfikacji zabezpieczeń kryptograficznych komunikacji sieciowej.	1
La8	Wykorzystanie kryptograficznych bibliotek programistycznych - Algorytm DES i AES.	2
La9	Implementacja algorytmu RSA.	2
La10	Wykorzystanie kryptograficznych bibliotek programistycznych - Algorytm RSA.	2
La11	Włączenie algorytmu RSA do aplikacji sieciowej.	1
La12	Implementacja podpisu cyfrowego w aplikacji sieciowej.	1
La13	Wykorzystanie certyfikatów kryptograficznych.	1
La14	Testy aplikacji wykorzystujących algorytmy kryptograficzne.	1
La15	Ocena postępów i wystawienie ocen końcowych.	1
	Suma godzin	18

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Wykład tradycyjny. N2. Laboratoria komputerowe. N3. Konsultacje dla studentów. N4. Praca własna – przygotowanie do laboratoriów. N5. Praca własna – samodzielne studia i przygotowanie do egzaminu.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEK_U01- PEK_U02	Punkty za wykonanie każdego zadania laboratoryjnego lub wykonanie każdej implementacji programowej.
P	PEK_U01- PEK_U02	Suma punktów F1. Aby zaliczyć, Student musi zdobyć ponad połowę punktów możliwych do uzyskania w trakcie semestru. Wykładowca może przyznać dodatkowe punkty za aktywność w trakcie zajęć w ciągu semestru.
P	PEK_W01 - PEK_W02	Egzamin. Aby zaliczyć, Student musi zdobyć ponad połowę punktów możliwych

		do uzyskania w trakcie egzaminu. Wykładowca może przyznać dodatkowe punkty za aktywność w trakcie wykładów w ciągu semestru.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych, Helion, 2012.
[2] Bauer F.L., Sekrety kryptografii. Helion, Gliwice, 2003.
[3] Koblitz N.: Wykład z teorii liczb i kryptografii, WNT, Warszawa, 2006.
[4] Koblitz N.: Algebraiczne aspekty kryptografii, WNT, Warszawa, 2000.
[5] Schneier B.: Kryptografia dla praktyków – Protokoły, algorytmu i programy źródłowe w języku C. WNT, Warszawa, 2002.

LITERATURA UZUPEŁNIAJĄCA:

[1] Kahn D.: Łamacze kodów, WNT, Warszawa, 2004.
[2] Ogiela M.: Systemy utajniania informacji, Uczelniane Wyd. AGH, Kraków, 2003.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Krzysztof Chudzik, Krzysztof.Chudzik@pwr.wroc.pl

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Kryptografia
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU **Informatyka**
I SPECJALNOŚCI **Bezpieczeństwo i Niezawodność Systemów Informatycznych**

Przedmiotowy efekt kształcenia	Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)**	Cele przedmiotu***	Treści programowe***	Numer narzędzia dydaktycznego***
PEK_W01 (wiedza)	K2INF_W01	C1	Wy1-Wy15	N1,3,5
PEK_W02	K2INF_W05, K2INF_W06	C2	Wy1-Wy15	N1,3,5
PEK_U01 (umiejętności)	K2INF_W01, K2INF_W05	C1, C2	La2-La15	N2,3,4
PEK_U02	K2INF_U09		La1	N2

** - wpisać symbole kierunkowych/specjalnościowych efektów kształcenia
*** - z tabeli powyżej