WYDZIAŁ MATEMATYKI
KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim:	**Kryptografia i bezpieczeństwo komputerowe**
Nazwa przedmiotu w języku angielskim:	**Cryptography and Computer Security**
Kierunek studiów:	**Matematyka**
Specjalność:	**Matematyka informatyczna**
Stopień studiów i forma:	**I stopień, stacjonarna**
Rodzaj przedmiotu:	**Wybieralny**
Kod przedmiotu:	
Grupa kursów:	**TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	**30**		**15**		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	**90**		**60**		
Forma zaliczenia	**zaliczenie na ocenę**				
Dla grupy kursów zaznaczyć kurs końcowy (X)	**X**				
Liczba punktów ECTS	**3**		**2**		
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)			**2**		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	**1,1**		**0,6**		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

CELE PRZEDMIOTU

C1. Przedstawianie podstawowych zagrożeń w systemach informacyjnych
C2. Zapoznanie słuchaczy podstawowych technik ochrony informacji

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy:
PEU_W01 Zna podstawowe zagrożenia w systemach informacyjnych
PEU_W02 Zna podstawowe mechanizmy ochrony danych

Z zakresu umiejętności:
PEU_U01 Umie stosować mechanizmy ochrony danych
PEU_U02 Umie wskazywać zagrożenia w przetwarzania danych
Z zakresu kompetencji społecznych:
PEU_K01 Potrafi identyfikować zagrożenia bezpieczeństwa w systemach rzeczywistych

TREŚCI PROGRAMOWE		
Forma zajęć - wykład		**Liczba godzin**
Wy1	Podstawowe pojęcia kryptografii i bezpieczeństwa informacji. Proste szyfry.	2
Wy2	Funkcje haszujące, integralność informacji	2
Wy3	Kryptografia symetryczna, szyfry blokowe	2
Wy4	Ataki na protokoły kryptografii symetrycznej	2
Wy5	Kryptografia asymetryczna. Algorytm RSA, problem faktoryzacji	2
Wy6	Problem dyskretnego logarytmu. Szyfr ElGamala	2
Wy7	Uwierzytelnianie kryptograficzne i biometryczne	2
Wy8	Protokoły z wiedzą zerową, przekaz nierozróżnialny	2
Wy9	Podpisy cyfrowe – podstawowe konstrukcje	2
Wy10	Podpisy cyfrowe o rozszerzonych funkcjonalnościach	2
Wy11	Dzielenie sekretów, kryptografia grupowa	2
Wy12	Certyfikaty, infrastruktura klucza publicznego	2
Wy13	Znaki wodne	2
Wy14	Techniki ochrony prywatności	2
Wy15	Kryptowaluty	2
	Suma godzin	**30**

Forma zajęć - ćwiczenia		Liczba godzin
Lab1	Analiza prostych protokołów	2
Lab2	Szyfry blokowe – konstrukcja, analiza, ataki	3
Lab3	Kryptografia asymetryczna – szyfrowanie	3
Lab4	Podpisy cyfrowe	3
Lab5	Infrastruktura klucza publicznego	2
Lab6	Techniki ochrony prywatności	2
	Suma godzin	**15**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
N1. Tradycyjny wykład N2. Rozwiązywanie zadań N3. Dyskusje nad problemami

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
P kolokwium końcowe obejmujące wszystkie efekty uczenia się.		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
LITERATURA PODSTAWOWA:
[1] Jonathan Katz, Yehuda Lindell, Introduction to modern cryptography (3rd ed.), CRC Press 2020. [2] D. R. Stinson, Maura B. Paterson Cryptography: Theory and Practice (4th ed), CRC Press 2018.
LITERATURA UZUPEŁNIAJĄCA:
[1] A. Menezes, P. van Oorschot, S. Vanstone Handbook of applied cryptography, CRC Press, 1996
OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

Prof. dr hab. inż. Marek Klonowski
dr Marcin Michalski (marcin.k.michalski@pwr.edu.pl)

i.