"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Kryptoanaliza algorytmów blokowych	Cryptanalysis of Block Algorithms
Kod przedmiotu	WCYKSWSM_KAB.....KAB	
Język wykładowy	polski	
Profil studiów	ogólnoakademicki	
Forma studiów	studia stacjonarne	
Poziom studiów	wojskowe studia jednolite magisterskie	
Rodzaj przedmiotu	obowiązkowy	
Obowiązuje od naboru	2021/2022	

Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS

semestr	(x egzamin, + zaliczenie, # projekt)						punkty ECTS
	razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium	
IX	30+	20	4+	6+			3.0
razem		20	4	6			3.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 9 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne
Autor	dr inż. Michał Misztal
Jednostka odpowiedzialna za przedmiot	Insytut Matematyki i Kryptologii
Skrócony opis przedmiotu	• Wykład • Ćwiczenia • Laboratorium

Pełny opis przedmiotu (treści programowe)

lp.	Semestr IX temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Podstawy kryptoanalizy algorytmów blokowych.	2				
2	Podstawy kryptoanalizy różnicowej.	2	2			
3	Pojęcie charakterystyki. Ataki 1R, 2R, 3R. Charakterystyki iteracyjne. Parametr S/N.	2	2			
4	Kryptoanaliza różnicowa algorytmu DES zredukowanego do 3, 4, 6, 8 rund.	3		4		
5	Kryptoanaliza różnicowa pełnego DES'a.	1				
6	Podstawy kryptoanalizy liniowej wg Matsui.	2		2		
7	Kryptoanaliza liniowa wg Bihama.	2				
8	Techniki kryptoanalizy różnicowej. Różniczki niemożliwe.	2				
9	Techniki kryptoanalizy różnicowej. Ataki sumacyjne.	2				
10	Najnowsze ataki: atak typu bumerang i prostokąt, atak z poślizgiem.	2				
	Razem	20	4	6		

Literatura

podstawowa:
- B. Schneier "Kryptografia dla praktyków", wyd. II, WNT 2002
- E. Biham, A. Shamir "Differential Cryptanalysis of the Data Encryption Standard" Springer-Verlag 1993

uzupełniająca:
- M. Matsui "Cryptanalysis Method for DES Cipher" EuroCrypt 1993
- H. M. Heys "A Tutorial on Linear and Differential Cryptanalysis", Memorial University of Newfoundland, Canada, 2001.

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
U1	Nauczyć podstaw kryptoanalizy szyfrów blokowych	K_W06 K_K01 K_W22
U2	Nauczyć zasady działania podstawowych metod ataków na szyfry blokowe	K_U11 K_U18 K_W06
W1	Zapoznać z podstawowymi technikami kryptoanalizy różnicowej oraz z praktycznymi atakami na wybrane szyfry blokowe	K_W14 K_W08

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)

- Zaliczenie w formie pisemnej
- Efekty U1, U2 i W2 sprawdzane są zaliczeniem pisemnym.

Bilans ECTS (nakład pracy studenta)

SEMESTR 9		
Aktywność	**Obciążenie studenta**	
	Liczba godzin	**Liczba ECTS**
Udział w wykładach	20	1

	SEMESTR 9		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w laboratoriach	6	0.5
	Udział w ćwiczeniach	4	0.5
	Udział w projektach	0	0
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	30	0.5
	Samodzielne przygotowanie do laboratoriów	20	0.25
	Samodzielne przygotowanie do ćwiczeń	20	0.25
	Samodzielna realizacja projektu		
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach		
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia	3	
	Udział w egzaminie / kolokwium	2	
	Sumaryczne obciążenie pracą studenta	105	3
	Zajęcia z udziałem nauczycieli	32	2
	Zajęcia powiązane z działalnością naukową	100	3
	Zajęcia o charakterze praktycznym	50	1.5

autor

dr inż. Michał Misztal
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr hab. Kojdecki Marek
tytuł, stopień naukowy, imię, NAZWISKO, podpis