"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Kryptoanaliza algorytmów strumieniowych	Cryptanalysis of Stream Ciphers
Kod przedmiotu	WCYKSWSM_KAS.....KAS	
Język wykładowy	polski	
Profil studiów	ogólnoakademicki	
Forma studiów	studia stacjonarne	
Poziom studiów	wojskowe studia jednolite magisterskie	
Rodzaj przedmiotu		
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	44+	24		20+			4.0
razem		24		20			4.0

Przedmioty wprowadzające
- Brak przedmiotów kształcenia wprowadzających

Semestr/kierunek studiów: semestr 9 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne

Autor: mgr inż. Krzysztof Mańk

Jednostka odpowiedzialna za przedmiot: WCY / IMK / LBK

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	odstawy kryptoanalizy szyfrów strumieniowych.	2				
2	Atak na złożoność liniową generatora.	2		2		
3	Kryptoanalityczne modele generatora klucza. Podstawy ataków korelacyjnych.	2		2		
4	Podstawowy atak korelacyjny Sigenthalera.	2		2		
5	Szybkie ataki korelacyjne.	4		4		
6	zybkie ataki korelacyjne. Znajdowanie równań "parity-checks".	4		4		
7	Atak na generator z filtrem.	2		2		
8	Atak na generator z sumacyjny.	2		2		
9	Atak na generatory z kontrolowanym zegarem.	2		2		
10	Kryptoanaliza wybranych algorytmów strumieniowych: LILI, A5.	2				
	Razem	24		20		

Literatura

podstawowa:
- B. Schneier "Kryptografia dla praktyków" wyd. II WNT 2002
- A. Menezes, P. van Orschote, S. Vanstone "Kryptografia stosowana" WNT 2005

uzupełniająca:
- R. A. Rueppel "Analysis and Design of Stream Ciphers" 1986

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
U1	Potrafi posługiwać się atakami korelacyjnymi	K_U18
U2	Potrafi samodzielnie pozyskiwać informacje, dokonać ich oceny i określić kierunki dalszego uczenia się	K_K01 K_U18 K_U18
W1	Ma ogólną wiedzę dotyczącą podstaw kryptoanalizy szyfrów strumieniowych	K_W06
W2	Ma wiedzę na temat różnych technik ataków na algorytmy strumieniowe	K_W06 K_W08 K_W14 K_U11 K_W22

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)
- Egzamin w formie pisemnej

Bilans ECTS (nakład pracy studenta)	SEMESTR 9		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	24	1
	Udział w laboratoriach	20	1
	Udział w ćwiczeniach	0	0
	Udział w projektach	0	0
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	24	1
	Samodzielne przygotowanie do laboratoriów	30	1
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu		
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach		
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia		
	Udział w egzaminie / kolokwium	2	
	Sumaryczne obciążenie pracą studenta	100	4
	Zajęcia z udziałem nauczycieli	46	2
	Zajęcia powiązane z działalnością naukową	98	4
	Zajęcia o charakterze praktycznym	50	2

autor

mgr inż. Krzysztof Mańk
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

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