"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Ataki algebraiczne	Algebraic Attacks
Kod przedmiotu	WCYKSWSM_AAG.....AAG	
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		10+			3.0
razem		20		10			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	Wydział Cybernetyki/Instytut Matematyki i Kryptologii/Zakład Podstaw Kryptografii i Kryptoanalizy
Skrócony opis przedmiotu	• Wykłady • Laboratoria

Pełny opis przedmiotu (treści programowe)

lp.	Semestr IX temat/tematyka zajęć	liczba godzin				
		wkł.	ćw.	lab.	prj.	sem.
1	Algebraiczne aspekty kryptografii symetrycznej. Wprowadzenie do przedmiotu.	4				
2	Istnienie równań do ataków algebraicznych. Anihilatory funkcji boolowskich. Odporność algebraiczna.	2		2		
3	Konstrukcja równań dla szyfrów strumieniowych i blokowych.	2		2		
4	Metody rozwiązywania układów równań. Algorytm XL i jego pochodne.	2		2		
5	Metody rozwiązywania układów równań. Algorytm ElimLin.	2				
6	Metody rozwiązywania układów równań. Bazy Groebnera.	4		2		
7	Metody rozwiązywania układów równań. SAT-solwery.	2		2		
8	Atak metodą kostek.	2				
	Razem	20		10		

Literatura

podstawowa:
- Schneier B., Kryptografia dla praktyków , wyd. II, 2002
- Rosen K.H., Elementary number theory and its applications , 1992
- Bard G. v., Algebraic Cryptanalysis, Springer Science+Business Media, LLC 2009

uzupełniająca:
- Szmidt J., Misztal M., Wstęp do kryptologii , Skrypt WSIZIS, Warszawa 2003

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W1	Ma wiedzę na temat metod i narzędzi do rozwiązywania układów równań.	K_W02
W2	Ma wiedzę na temat podstaw kryptoanalizy szyfrów blokowych i strumieniowych z wykorzystaniem metod algebraicznych.	K_W02
W3	Zapoznał się z dostępnymi pakietami umożliwiającymi rozwiązywanie układów równań.	K_U03
U1	Potrafi dokonać krytycznej analizy szyfrów blokowych i strumieniowych pod kątem podatności na ataki algebraiczne.	K_W02 K_U11
U2	Potrafi pozyskiwać informacje z literatury, w tym głównie w języku angielskim.	K_U11

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Moduł kształcenia zaliczany jest na podstawie: zaliczenia • Warunkiem koniecznym do uzyskania zaliczenia laboratorium jest udział w co najmniej 80% zajęć. • Zaliczenie przeprowadzane jest w formie pisemnej. Podczas zaliczenia można korzystać z materiałów. • Efekty W1, W2, U1 sprawdzane są na zaliczeniu przedmiotu. • Efekty W1, W3, U1, U2 sprawdzane są na laboratoriach.

Bilans ECTS (nakład pracy studenta)

SEMESTR 9		
Aktywność	**Obciążenie studenta**	
	Liczba godzin	**Liczba ECTS**
Udział w wykładach	20	1
Udział w laboratoriach	10	1
Udział w ćwiczeniach	0	0
Udział w projektach	0	0
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów	20	0.5
Samodzielne przygotowanie do laboratoriów	30	0.5
Samodzielne przygotowanie do ćwiczeń		
Samodzielna realizacja projektu		
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach		
Przygotowanie do egzaminu		
Przygotowanie do zaliczenia		
Udział w egzaminie / kolokwium		
Sumaryczne obciążenie pracą studenta	80	3
Zajęcia z udziałem nauczycieli	30	2
Zajęcia powiązane z działalnością naukową	80	3
Zajęcia o charakterze praktycznym	40	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