

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Narzędzia kryptoanalizy					Tools of cryptanalysis		
Kod przedmiotu	WCYKSCSI							
Język wykładowy	polski							
Profil studiów	ogólnoakademicki							
Forma studiów	studia stacjonarne							
Poziom studiów	studia pierwszego stopnia							
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	
	VI	44+	20		24+			4.0
	razem		20		24			4.0
Przedmioty wprowadzające	• Elementy teorii liczb - K_W02, K_W22 • Krzywe eliptyczne - K_U18, K_W02, K_W22, K_W23 • Wstęp do kryptoanalizy klucza publicznego - K_U18, K_W02, K_W22 • Wybrane elementy kryptologii - K_U03, K_U17, K_W02							
Semestr/kierunek studiów	semestr 6 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne							
Autor	dr inż. Michał Wroński							
Jednostka odpowiedzialna za przedmiot	WCY/IMK/LBK							
Skrócony opis przedmiotu	• Przedmiot zaliczany jest na podstawie zaliczenia sprawdzającego wiedzę (W01, W02) i umiejętności (U01, U02). • Zaliczenie przeprowadzany jest w formie pisemnej lub pisemnej i ustnej. • Laboratoria zaliczane są na podstawie wyników pracy na zajęciach, w formie zadań do samodzielnego rozwiązania (U01, U02). • Skala ocen: dostatecznie (3) - student zna i rozumie większość wyłożonych zagadnień, umie rozwiązywać najprostsze zadania, rozumie treść najważniejszych twierdzeń; dobrze (4) - student zna i rozumie znaczną większość wyłożonych zagadnień, umie formułować i rozwiązywać najprostsze zadania oraz interpretować ich wyniki za pomocą twierdzeń; bardzo dobrze (5) - student zna i rozumie wszystkie wyłożone zagadnienia, umie formułować i rozwiązywać zadania oraz interpretować ich wyniki za pomocą twierdzeń; dość dobrze (3, 5) i ponad dobrze (4,5) - pośrednio między dostatecznie i dobrze oraz między dobrze i bardzo dobrze.							
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VI temat/tematyka zajęć	liczba godzin					
			wkl.	ćw.	lab.	prj.	sem.	
	1	Wprowadzenie do przedmiotu. Omówienie podstawowych rodzajów ataków wykorzystujących matematyczne własności algorytmów oraz narzędzi służących do kryptoanalizy.	2					
	2	Wybrane ataki na krzywe eliptyczne I. Określenie podstawowych parametrów bezpiecznych kryptograficznie krzywych eliptycznych. Modele krzywych eliptycznych. Redukcja Pohliga-Hellmana.	2					
	3	Wybrane ataki na krzywe eliptyczne II. Atak na krzywe anomalne. Atak MOV.	2					
	4	Ataki wykorzystujące błędy w implementacji. Metody drabiny. Arytmetyka jednorodna. Arytmetyka kompletna. Ataki z błędami.	2					
	5	Funkcje skrótu i KDF. Sposoby odzyskiwania haseł na podstawie skrótu.	2					
	6	Idea ataków algebraicznych. Sposób generacji równań opisujących algorytm. SAT solvery.	2					
	7	Ataki kwantowe z wykorzystaniem komputera kwantowego ogólnego przeznaczenia. Algorytm Shor'a.	2					
	8	Ataki kwantowe wykorzystujące wyżarzanie kwantowe. Problemy optymalizacyjne QUBO oraz Ising. Przekształcenie problemu faktoryzacji do problemu QUBO.	2					
	9	Ataki kwantowe wykorzystujące wyżarzanie kwantowe. Przekształcenie problemu logarytmu dyskretnego do problemu QUBO.	2					
	10	Zaliczenie.	2					
11	Implementacja ataku na krzywe anomalne oraz ataku MOV.			4				

	lp.	Semestr VI temat/tematyka zajęć	liczba godzin				
			wkl.	ćw.	lab.	prj.	sem.
	12	Implementacja drabin i arytmetyki jednorodnej (kompletnej). Implementacja wybranego ataku z błędami.			4		
	13	Wykorzystanie programu Hashcat do odzyskiwania haseł na podstawie skrótów.			4		
	14	Generacja równań opisujących wybrany algorytm kryptograficzny.			4		
	15	Implementacja algorytmu Shor'a w wybranym symulatorze komputera kwantowego.			4		
	16	Transformacja problemu faktoryzacji do problemu QUBO i rozwiązanie go w wybranym środowisku.			4		
	Razem		20		24		
Literatura	podstawowa: ● I. Blake, G. Seroussi, N. Smart, Krzywe eliptyczne w kryptografii, WNT, 2004. ● M. Hirvensalo, Quantum Computing, Springer-Verlag 2004. ● F. Glover, G. Kochenberger, Y. Du, A Tutorial on Formulating and Using QUBO Models. arXiv Archive, arXiv: 1811.11538. ● G. Bard, Algebraic Cryptanalysis, Springer-Verlag, 2009. uzupełniająca: ● J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 2009. ● L. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition, CRC Press, 2008.						
Efekty uczenia się	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku				
	W01	Posiada podstawową wiedzę na temat podstawowych ataków teoretycznych na wybrane kryptosystemy	K_W22, K_W23				
	W02	Posiada podstawową wiedzę na temat ataków wynikających z błędów implementacyjnych wybranych kryptosystemów	K_W23				
	U01	Umie formułować i projektować ataki z wykorzystaniem podstawowych narzędzi służących do kryptoanalizy	K_U18				
	U02	Umie implementować ataki z wykorzystaniem podstawowych narzędzi służących do kryptoanalizy	K_U18				
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	● Przedmiot zaliczany jest na podstawie zaliczenia sprawdzającego wiedzę (W01, W02) i umiejętności (U01, U02). ● Zaliczenie przeprowadzany jest w formie pisemnej lub pisemnej i ustnej. ● Laboratoria zaliczane są na podstawie wyników pracy na zajęciach, w formie zadań do samodzielnego rozwiązania (U01, U02). ● Skala ocen: dostatecznie (3) - student zna i rozumie większość wyłożonych zagadnień, umie rozwiązywać najprostsze zadania, rozumie treść najważniejszych twierdzeń; dobrze (4) - student zna i rozumie znaczną większość wyłożonych zagadnień, umie formułować i rozwiązywać najprostsze zadania oraz interpretować ich wyniki za pomocą twierdzeń; bardzo dobrze (5) - student zna i rozumie wszystkie wyłożone zagadnienia, umie formułować i rozwiązywać zadania oraz interpretować ich wyniki za pomocą twierdzeń; dość dobrze (3, 5) i ponad dobrze (4,5) - pośrednio między dostatecznie i dobrze oraz między dobrze i bardzo dobrze.						
Bilans ECTS (nakład pracy studenta)	SEMESTR 6						
	Aktywność		Obciążenie studenta				
			Liczba godzin	Liczba ECTS			
	Udział w wykładach		20	1			
	Udział w laboratoriach		24	1			
	Udział w ćwiczeniach		0	0			
	Udział w projektach		0	0			
	Udział w seminariach		0	0			
	Samodzielne studiowanie tematyki wykładów		30	1			
	Samodzielne przygotowanie do laboratoriów		40	1			
	Samodzielne przygotowanie do ćwiczeń						
	Samodzielna realizacja projektu						
	Samodzielne przygotowanie do seminariów						
	Udział w konsultacjach						
	Przygotowanie do egzaminu						
	Przygotowanie do zaliczenia		5				
	Udział w egzaminie / kolokwium						
	Sumaryczne obciążenie pracą studenta		119	4			
	Zajęcia z udziałem nauczycieli		44				

	SEMESTR 6		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Zajęcia powiązane z działalnością naukową	114	4
	Zajęcia o charakterze praktycznym	64	2

autor

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

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

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