"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Wstęp do kryptoanalizy klucza publicznego	Introduction to Public Key Cryptanalysis
Kod przedmiotu	WCYKSWSM_.....	
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	
VII	30x	14		16+			3.0
razem		14		16			3.0

Przedmioty wprowadzające

- Matematyka dyskretna I -
- Matematyka dyskretna II -
- Matematyka I -
- Matematyka II -
- Matematyka III -
- Wprowadzenie do programowania -

Semestr/kierunek studiów	semestr 7 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne
Autor	dr Mariusz Jurkiewicz
Jednostka odpowiedzialna za przedmiot	WCY/IMiK/LBK
Skrócony opis przedmiotu	• Wykład • Laboratorium

Pełny opis przedmiotu (treści programowe)

lp.	Semestr VII temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Powstanie i ewolucja kryptologii klucza publicznego; Małe twierdzenie Fermata, Twierdzenie Eulera, RSA i Twierdzenie o poprawności RSA; Problem faktoryzacji	2		1		
2	Ułamki łańcuchowe; Atak na RSA z małym kluczem prywatnym (atak diofantyczny).	2		3		
3	Algorytm faktoryzacji p-1 Pollard'a; Liczby gładkie; Sito Kwadratowe; Faktoryzacja metodą różnicy kwadratów.	2		2		
4	Paradoks dnia urodzin; Twierdzenie o kolizjach; Zastosowanie twierdzenia o kolizjach do ataków na problem logartymu dyskretnego. Pewne ataki kolizyjne; Algorytm Shanks'a.	2		2		
5	Metoda rho Pollard'a wraz z jej związkami z teorią dyskretnych układów dynamicznych.	2		3		
6	Metoda indeksu	2		3		
7	Algorytm Pohling'a-Hellman'a oraz jego zastosowania.	2		2		
	Razem	14		16		

Literatura

podstawowa:

- J. Katz, Y. Lindell, Introduction to modern cryptography, CEC Press, 2015.
- B. Schneier, Kryptografia dla praktyków, WNT, 2002.
- S. D. Galbraith, Mathematics of public key cryptography, Cambridge University Press, 2012.

uzupełniająca:

- M. J. Hinek, Cryptoanalysis of RSA and its variants, CRC Press, 2010.
- H. Cohen, G. Frey, Handbook of elliptic and hyperelliptic curve cryptography, Chapman & Hall/CRC, 2006.

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W01	Ma uporządkowaną, podbudowaną teoretycznie wiedzę dotyczącą zasadniczych problemów klasycznej (nie postkwantowej) kryptologii asymetrycznej	K_W02
W02	Ma wiedzę z zakresu metod kryptoanalizy wybranych algorytmów klucza publicznego opartych o problem faktoryzacji oraz DLP.	K_U19, K_W02, K_W22
U01	Umie posługiwać się w podstawowym zakresie językiem	K_U19, K_W22

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
		kryptologii asymetrycznej, wykorzystując właściwe określenia i symbole. Umie dokonać próby ataku na wybrane algorytmy asymetryczne	
	U02	Umie wykonać podstawową analizę bezpieczeństwa algorytmów opartych o klasyczne problemy klucza publicznego i udokumentować wyniki.	K_U19, K_W02, K_W22
	U03	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie.	K_U19, K_W02, K_W22

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

- Przedmiot zaliczany jest na podstawie egzaminu sprawdzającego wiedzę (W01 i W02) i umiejętności (U01).
- Egzamin przeprowadzany jest w formie pisemnej lub ustnej.
- Warunkiem dopuszczenia do egzaminu jest zaliczenie laboratorium oraz obecność na co najmniej 87.5% zajęć. Laboratoria zaliczane są na podstawie wyników prac wykonywanych pod bezpośrednią kontrolą podczas zajęć (U01, U02, W01, W02) oraz projektu końcowego (U01, U02, U03). Dodatkowo studenci otrzymują wskazówki do samodzielnego studiowana z zachętą do korzystania z różnorodnych źródeł wiedzy (U03 i K01).
- Skala ocen: dostatecznie (3) - student zna i rozumie większość wyłożonych zagadnień, umie rozwiązywać najprostsze problemy; dobrze (4) - student zna i rozumie znaczną większość wyłożonych zagadnień, umie rozwiązywać najprostsze problemy oraz interpretować ich wyniki; bardzo dobrze (5) - student zna i rozumie wszystkie wyłożone zagadnienia, umie rozwiązywać postawione problemy oraz interpretować ich wyniki; 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 7

Aktywność	Obciążenie studenta	
	Liczba godzin	Liczba ECTS
Udział w wykładach	14	0.5
Udział w laboratoriach	16	0.35
Udział w ćwiczeniach	0	0
Udział w projektach	0	0.3
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów	20	0.25
Samodzielne przygotowanie do laboratoriów	15	0.25
Samodzielne przygotowanie do ćwiczeń		
Samodzielna realizacja projektu	10	0.45
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach	2	0.1
Przygotowanie do egzaminu	10	0.35
Przygotowanie do zaliczenia	8	0.35
Udział w egzaminie / kolokwium	2	0.1
Sumaryczne obciążenie pracą studenta	97	3
Zajęcia z udziałem nauczycieli	34	1.35
Zajęcia powiązane z działalnością naukową	75	2.1
Zajęcia o charakterze praktycznym	41	1.35

autor

dr Mariusz Jurkiewicz

tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr hab. Kojdecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis