"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Elements of Public-Key Cryptology (w języku angielskim)	Elements of Public-Key-Cryptology
Kod przedmiotu	WCYKSWSM_.....	
Język wykładowy	angielski	
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	
X	30x	20		10+			3.0
razem		20		10			3.0

Przedmioty wprowadzające

- Teoretyczne podstawy informatyki -
- Język angielski -
- Wstęp do kryptologii -

Semestr/kierunek studiów: semestr 10 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne

Autor: dr Mariusz Jurkiewicz

Jednostka odpowiedzialna za przedmiot: WCY/IMiK/LBK

Skrócony opis przedmiotu

- Wykład
- Labolatorium

Pełny opis przedmiotu (treści programowe)

lp.	Semestr X temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Introductory material; principles of modern cryptography; notion of security model; RMA, KMA, CMA -security; classical oracle model; random oracle model	4				
2	Relations between RMA-security and CMA-secutiry; Relations between KMA-security and CMA-secutiry	4				
3	Notion of KMA-security of one-time DSS; Transformation of KMA-secure DSS to CMA-secure DSS	4				
4	Simple transform to convert CMA-secure DSSs to strongly CMA-secure DSSs	2				
5	Security of W-OTS+ DSS.	2				
6	Introductory analysis of provably secure Lamport-Diffie one-time DSS; Hash functions in modern cryptography	4		4		
7	Implementation of provably secure Lamport-Diffie one-time DSS; Security analysis of Lamport-Diffie one-time DSS			4		
8	Hash functions in modern cryptography			2		
	Razem	20		10		

Literatura

podstawowa:

- Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, Chapman & Hall/CRC Cryptography and Network Security, 2nd Edition
- Mihir Bellare, Phillip Rogaway, Introduction to Modern Cryptography - https://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf
- https://eprint.iacr.org

uzupełniająca:

- https://eprint.iacr.org

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W01	Ma uporządkowaną, podbudowaną teoretycznie wiedzę dotyczącą różnych rodzajów pojęcia podpisu elektronicznego oraz dedykowanych im różnych modeli bezpieczeństwa. Potrafi posługiwać się angielskim słownictwem w tym zakresie.	K_U02, K_W22,
W02	Ma wiedzę z zakresu różnych metod redukcji, służących od przeprowadzenia dowodów bezpieczeństwa schematów podpisów elektronicznych w modelu klasycznym bez losowej wyroczni. Potrafi posługiwać się angielskim słownictwem w tym zakresie.	K_U02, K_W02, K_W22

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
	U01	Umie wykonać proste dowody bezpieczeństwa schematów w modelu klasycznym.	K_U02, K_U11, K_W02

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 90% zajęć. Laboratoria zaliczane są na podstawie wyników prac wykonywanych pod bezpośrednią kontrolą podczas zajęć (U01, W01, W02) oraz projektu końcowego (U01). Dodatkowo studenci otrzymują wskazówki do samodzielnego studiowana z zachętą do korzystania z różnorodnych źródeł wiedzy.
- 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 10

Aktywność	Obciążenie studenta	
	Liczba godzin	Liczba ECTS
Udział w wykładach		0.5
Udział w laboratoriach		0.35
Udział w ćwiczeniach		
Udział w projektach		0.3
Udział w seminariach		
Samodzielne studiowanie tematyki wykładów	25	0.25
Samodzielne przygotowanie do laboratoriów	20	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	15	0.35
Przygotowanie do zaliczenia	8	0.35
Udział w egzaminie / kolokwium	2	0.1
Sumaryczne obciążenie pracą studenta	82	3
Zajęcia z udziałem nauczycieli	4	1.35
Zajęcia powiązane z działalnością naukową	55	2.1
Zajęcia o charakterze praktycznym	30	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