SYLABUS PRZEDMIOTU

Kryptografia Post-Kwantowa

I. Informacje ogólne

Nazwa przedmiotu	*Kryptografia Post-Kwantowa*
Kod przedmiotu 06-	KRP
Rodzaj przedmiotu:	specjalistyczny
Kierunek studiów:	Informatyka
Poziom kształcenia:	II stopień
Profil kształcenia:	Ogólnoakademicki
Rok studiów:	drugi
Rodzaje zajęć i liczba godzin	
Wykład	0
Ćwiczenia	15
Laboratoria	15
Praktyki	0
Liczba punktów ECTS 3	

Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/ prowadzących zajęcia

- Prof. UAM dr hab. Maciej Grześkowiak maciejg@amu.edu.pl

Język wykładowy	polski
Przedmiot prowadzony zdalnie (e-learning)	tak, częściowo

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- prezentacja algorytmów i protokołów kryptologicznych odpornych na ataki z wykorzystaniem komputera kwantowego,

- nabycie umiejętności analizowania bezpieczeństwa systemu informatycznego,

- umiejętność wykorzystania aparatu matematycznego w procesie analizy i tworzenia systemu informatycznego,

- prezentacja modelu komputera kwantowego i algorytmów kwantowych,

2. Wymagania wstępne w zakresie wiedzy, umiejętności oraz kompetencji społecznych

Umiejętność programowania na poziomie inżyniera informatyki.

Znajomość podstaw algebry na poziomie inżyniera informatyki.

Znajomość kryptologii na poziomie studiów II stopnia.

3. Efekty uczenia się (EU) dla zajęć i odniesienie do efektów uczenia się (EK) dla kierunku studiów

Symbol EU dla przedmiotu	Symbol EK dla kierunku studiów	Po zakończeniu modułu i potwierdzeniu osiągnięcia EU student/ka:
KRP_01	KINF2_W02 KINF2_U09 KINF2_K02	Zna współczesną terminologię kryptologiczną.
KRP_02	KINF2_W02 KINF2_W05 KINF2_K01	Zna model matematyczny komputera kwantowego oraz rozumie zasadę działania podstawowych algorytmów kwantowych.
KRP_03	KINF2_W04 KINF2_U04 KINF2_U07	Umie analizować bezpieczeństwo protokołów kryptologicznych odpornych na ataki z wykorzystaniem komputera kwantowego.
KRP_04	KINF2_U04 KINF2_U07	Potrafi ocenić zagrożenia dla bezpieczeństwa systemu informatycznego wynikające z budowy komputera kwantowego.
KRP_05	KINF2_W03 KINF2_W05	Potrafi efektywnie implementować systemy kryptologiczne.
KRP_06	KINF2_W02	Potrafi wykorzystać w implementacji istniejące biblioteki kryptograficzne.

KRP_07	KINF2_W01 KINF2_W05 KINF2_K01	Wykorzystuje twierdzenia matematyczne w analizie systemów kryptograficznych.
KRP_08	KINF2_W04 KINF2_U04 KINF2_U07	Rozumie zagrożenia wynikające z niewłaściwego wykorzystania technik kryptologicznych.
KRP_09	KINF2_W02 KINF2_W03 KINF2_U11 KINF2_U08	Zna i rozumie współczesne rekomendacje systemów kryptologicznych odpornych na ataki z wykorzystaniem komputera kwantowego.
KRP_10	KINF2_W01 KINF2_W05 KINF2_U12 KINF2_K01 KINF2_K05	Rozwija swoje kompetencje matematyczne w zakresie informatyki.

4. Treści programowe zapewniające uzyskanie efektów uczenia się (EU) z odniesieniem do odpowiednich efektów uczenia się (EU) dla przedmiotu

Lp.	Symbol EU dla przedmiotu	Godzin Wykład	Godzin ĆW/ LAB/ SEM	Godzin pracy własnej	Opis treści kształcenia modułu zajęć/przedmiotu
Suma		30	30	90	
1.	KRP_05 KRP_06 KRP_07 KRP_10		2	3	Ciała skończone i ich implementacja.
2.	KRP_07 KRP_10		2	3	Krzywe eliptyczne nad ciałami skończonymi.
3.	KRP_07 KRP_10		2	3	Izogenie krzywych eliptycznych. Grafy izogenii.
4.	KRP_01 KRP_07 KRP_10		2	3	Protokół wymiany klucza SIDH.
5.	KRP_01 KRP_07 KRP_09		2	3	Supersingular Isogeny Key Encapsulation (SIKE).
6.	KRP_05 KRP_06		2	3	Aspekty implementacyjne SIKE.
7.	KRP_01 KRP_09		2	3	Przegląd rekomendacji NIST dotyczących systemów post-kwantowych.
8.	KRP_02 KRP_07 KRP_10		2	3	Model komputera kwantowego oraz wprowadzenie do obliczeń i algorytmów kwantowych.
9.	KRP_05 KRP_06		2	3	Qiskit - open source quantum development.
10.	KRP_02 KRP_07 KRP_10		2	3	Algorytm Grovera.
11.	KRP_02 KRP_07		2	3	Algorytm Simona.

	KRP_10				
12.	KRP_01 KRP_03 KRP_04 KRP_08		2	3	Kwantowe ataki na symetryczne systemy szyfrowe.
13.	KRP_02 KRP_07 KRP_10		2	3	Algorytm oszacowania fazy.
14.	KRP_02 KRP_07 KRP_10		2	3	Algorytm Shora.
15.	KRP_01 KRP_03 KRP_04 KRP_08		2	3	Kwantowe ataki na asymetryczne systemy szyfrowe.

5. Zalecana literatura

1) D. Bernstein, J. Buchmann, E. Dahmen, ,,Post –Quantum Cryptography", Springer, 2009.
2) M. Hirvensalo, ,,Quantum computing', Springer, 2004.
3) Luca De Feo, ,,Mathematics of Isogeny Based Cryptography", arXiw, 2017.

III. Informacje dodatkowe

1. Metody i formy prowadzenia zajęć umożliwiające osiągnięcie założonych EU (proszę wskazać z proponowanych metod właściwe dla opisywanych zajęć lub/i zaproponować inne)

Realizacja	Metody i formy prowadzenia zajęć
	Wykład z prezentacją multimedialną wybranych zagadnień
	Wykład konwersatoryjny
	Wykład problemowy
	Dyskusja
	Praca z tekstem
	Metoda analizy przypadków
	Uczenie problemowe (Problem-based learning)
	Gra dydaktyczna/symulacyjna
✔	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych)
✔	Metoda ćwiczeniowa
✔	Metoda laboratoryjna
	Metoda badawcza (dociekania naukowego)
	Metoda warsztatowa
	Metoda projektu
	Pokaz i obserwacja
	Demonstracje dźwiękowe i/lub video
	Metody aktywizujące (np.: „burza mózgów", technika analizy SWOT, technika drzewka decyzyjnego, metoda „kuli śniegowej", konstruowanie „map myśli")
	Praca w grupach
	Wykład zdalny w czasie rzeczywistym

	Wykład zdalny asynchroniczny uzupełniony spotkaniem w czasie rzeczywistym
	Wykład zdalny asynchroniczny z aktywnością studenta uzupełniony spotkaniem w czasie rzeczywistym
✔	Ćwiczenia/laboratoria/konwersatoria zdalne w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą indywidualną studenta uzupełnione spotkaniem w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą grupową studentów uzupełnione spotkaniem w czasie rzeczywistym
	Laboratorium cyfrowe zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Konwersatorium asynchroniczne zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Seminarium zdalne w czasie rzeczywistym
	Seminarium asynchroniczne zdalne ze spotkaniem w czasie rzeczywistym
	Inne (jakie?) -

2. Sposoby oceniania stopnia osiągnięcia EU (proszę wskazać z proponowanych sposobów właściwe dla danego EU lub/i zaproponować inne

Sposoby oceniania	Symbole EU dla modułu zajęć/przedmiotu									
	KRL: 01, 02, 03, 04, 05, 08, 09.	KRL: 06, 07.								
Egzamin pisemny										
Egzamin ustny										
Egzamin z „otwartą książką”										

Kolokwium pisemne	✔									
Kolokwium ustne										
Test	✔									
Projekt		✔								
Esej										
Raport										
Prezentacja multimedialna										
Egzamin praktyczny (obserwacja wykonawstwa)										
Portfolio										
Zadania cząstkowe na wykładzie										
...										

3. Nakład pracy studenta i punkty ECTS

Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (wg planu studiów) z nauczycielem		30
Praca własna studenta*	Przygotowanie do zajęć	5
	Czytanie wskazanej literatury	5
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	0
	Przygotowanie projektu	15
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	10
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	10
	Praca z laboratorium cyfrowym (np. Code Runner)	0
	Inne (jakie?)	
SUMA GODZIN		75
LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU		3

* proszę wskazać z proponowanych przykładów pracy własnej studenta właściwe dla opisywanego modułu lub/i zaproponować inne

4. Kryteria oceniania wg skali stosowanej w UAM

Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 83% punktów
dobry plus (+db; 4,5)	od 75% punktów
dobry (db; 4,0)	od 67% punktów
dostateczny plus (+dst; 3,5)	od 59% punktów
dostateczny (dst; 3,0)	od 50% punktów
niedostateczny (ndst; 2,0)	poniżej 50% punktów