SYLABUS PRZEDMIOTU

Kryptologia

I. Informacje ogólne

Nazwa przedmiotu	*Kryptologia*
Kod przedmiotu	KRY
Rodzaj przedmiotu:	specjalistyczny
Kierunek studiów:	Informatyka
Poziom kształcenia:	II stopień
Profil kształcenia:	Ogólnoakademicki
Rok studiów:	drugi
Rodzaje zajęć i liczba godzin	
Wykład	30
Ćwiczenia	15
Laboratoria	15
Praktyki	0
Liczba punktów ECTS	6

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 współczesnych algorytmów i protokołów kryptologicznych,

- poznanie charakterystyki bezpiecznego systemu informatycznego,

- nabycie umiejętności analizowania bezpieczeństwa systemu informatycznego,
- umiejętność wykorzystania aparatu matematycznego w procesie analizy i tworzenia systemu informatycznego.

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

Umiejętność programowania na poziomie inżyniera informatyki.

Znajomość podstaw algebry na poziomie inżyniera informatyki.

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:
KRY_01	KINF2_W03 KINF2_U09	Zna współczesną terminologię kryptologiczną
KRY_02	KINF2_W05 KINF2_U05 KINF2_U07	Potrafi wskazać wady i zalety danego rozwiązania kryptologicznego.
KRY_03	KINF2_W05 KINF2_U05 KINF2_K01	Potrafi analizować bezpieczeństwo protokołów kryptologicznych.
KRY_04	KINF2_W01 KINF2_U01	Potrafi obliczyć złożoność obliczeniową algorytmów wykorzystywanych do konstrukcji systemów kryptologicznych.
KRY_05	KINF2_W04 KINF2_U04	Potrafi efektywnie implementować podstawowe systemy kryptologiczne.
KRY_06	KINF2_W03 KINF2_U02	Potrafi wykorzystać w implementacji istniejące biblioteki kryptograficzne.
KRY_07	KINF2_W01 KINF2_U01	Wykorzystuje twierdzenia matematyczne w analizie systemów kryptograficznych.
KRY_08	KINF2_W03 KINF2_U07	Rozumie zagrożenia wynikające z niewłaściwego wykorzystania technik kryptologicznych.

KRY_09	KINF2_W02 KINF2_W07 KINF2_U02 KINF2_K02	Zna i rozumie współczesne rekomendacje systemów kryptologicznych.
KRY_10	KINF2_W07 KINF2_U09	Zna współcześnie stosowane podstawowe protokoły i rozwiązania kryptograficzne.
KRY_11	KINF2_W02 KINF2_U04 KINF2_U08 KINF2_K02	Zna specyfikację standardów kryptologicznych.

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.	KRY_01	2		3	Wprowadzenie do kryptologii. Podstawowe protokoły kryptograficzne.
2.	KRY_04 KRY_07		2	3	Złożoność obliczeniowa. Funkcje jednokierunkowe.
3.	KRY_08 KRY_10	2		3	Symetryczne systemy szyfrowania. Szyfrowanie doskonałe. Szyfry blokowe.
4.	KRY_10 KRY_11		2	3	Advanced Encryption Standard (AES).
5.	KRY_02 KRY_03 KRY_04	2		3	Kryptoanaliza szyfrów blokowych.
6.	KRY_08 KRY_10		2	3	Szyfrowanie uwierzytelnione.
7.	KRY_08 KRY_10 KRY_11	2		3	Jednokierunkowe funkcje skrótu i ich zastosowanie.
8.	KRY_02 KRY_04		2	3	Ataki na jednokierunkowe funkcje skrótu.
10.	KRY_10 KRY_11	2		3	Generatory ciągów pseudolosowych. Szyfry strumieniowe.
11.	KRY_02 KRY_03 KRY_07		2	3	Kryptoanaliza szyfrów strumieniowych
12.	KRY_07 KRY_10 KRY_11	2		3	Asymetryczne systemy szyfrowania. Algorytm RSA. Szyfrowanie RSA-OAEP

13.	KRY_07 KRY_10 KRY_11		2	3	Algorytm ElGamala. Założenie Diffiego-Hellmana.
14.	KRY_07 KRY_02 KRY_03	2		3	Ataki na asymetryczne systemy szyfrowania
15.	KRY_10 KRY_11		2	3	Protokoły uzgadniania kluczy. Protokół Diffiego-Hellmana.
16.	KRY_05 KRY_06 KRY_11	2		3	Bibiloteka Openssl.
17.	KRY_07		2	3	Krzywe eliptyczne nad ciałem skończonym.
18.	KRY_10 KRY_07	2		3	Problem logarytmu dyskretnego na krzywej eliptycznej. Protokół ElGamala na krzywej eliptycznej.
19.	KRY_10 KRY_07		2	3	Protokół ECDH. Problem obliczeniowy DH i problem decyzyjny DH.
20.	KRY_05 KRY_07	2		3	Aspekty implementacyjne systemów opartych na krzywych eliptycznych.
21.	KRY_01 KRY_09 KRY_10 KRY_11		4	3	Rekomendacje NIST dotyczące krzywych eliptycznych.
22.	KRY_10 KRY_11	2		3	Schematy podpisów cyfrowych. Podpis cyfrowy RSA.
23.	KRY_10 KRY_11		2	3	Standard podpisu cyfrowego. Podpis ECDSA
24.	KRY_10 KRY_07	2		3	Protokoły związane z podpisami cyfrowymi. Ślepe podpisy. Kanał podprogowy.

25.	KRY_09 KRY_10		2	3	Protokoły uwierzytelniania. Protokół challenge and response.
26.	KRY_10 KRY_11	2		3	Dowody z wiedzą zerową. Protokół Schnorra.
27.	KRY_08 KRY_10		2	3	Certyfikaty. Infrastruktura klucza publicznego
28.	KRY_03 KRY_08 KRY_09 KRY_10 KRY_11	2		3	Protokół SSL.
29.	KRY_03 KRY_08 KRY_09 KRY_10 KRY_11		2	3	Protokół Kerberos.
30.	KRY_03 KRY_08 KRY_09 KRY_11	2		3	Kleptografia.

5. Zalecana literatura

1) Mirosław Kutyłowski, Willy-B. Strothmann, ,,Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych", Wydawnictwo READ ME, 1998.
2) Jonathan Katz, Yehuda Lindell, ,,Introduction to modern cryptography", Taylor & Francis Inc., 2014.
3) Neal Koblitz, ,,Wykład z teorii liczb i kryptografii", Wydawnictwa Naukowo-Techniczne, 1994.
4) William Stallings, ,,Cryptography and Network Security", Pearson Education, Inc, 2006.

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

	Symbole EU dla modułu zajęć/przedmiotu

Sposoby oceniania

	KRY: 01, 02, 03, 04, 07, 08, 09, 11.	KRY: 05, 06, 11.								
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		60
Praca własna studenta*	Przygotowanie do zajęć	20
	Czytanie wskazanej literatury	10
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	0
	Przygotowanie projektu	30
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	10
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	20
	Praca z laboratorium cyfrowym (np. Code Runner)	0
	Inne (jakie?)	
SUMA GODZIN		150
LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU		6

* 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


Fundusze
Europejskie
Polska Cyfrowa
Rzeczpospolita
Polska
Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego