Załącznik Nr 5 do Zarz. Nr 33/11/12

(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: ZAAWANSOWANE ASPEKTY KRYPTOGRAFII	**2. Kod przedmiotu: ZAK**
3. Karta przedmiotu ważna od roku akademickiego: 201S/2016	
4. Forma kształcenia: studia drugiego stopnia	
5. Forma studiów: studia niestacjonarne	
6. Kierunek studiów: INFORMATYKA (RAU)	
7. Profil studiów: ogólnoakademicki	
8. Specjalność: -	
9. Semestr: III	
10. Jednostka prowadząca przedmiot: Wydział Automatyki, Elektroniki i Informatyki	
11. Prowadzący przedmiot: dr inż. Jacek Lach	
12. Przynależność do grupy przedmiotów: przedmioty specjalnościowe	
13. Status przedmiotu: wybieralny	
14. Język prowadzenia zajęć: polski	
15. Przedmioty wprowadzające oraz wymagania wstępne: Programowanie komputerów, Algorytmy i Struktury Danych, Systemy operacyjne. Kryptografia i ochrona danych. Student powinien posiadać podstawową wiedzę z zakresu budowy i programowania komputerów, złożoności obliczeniowej algorytmów, budowy i działania systemów operacyjnych i sieci komputerowych. Pomocna będzie znajomość podstawowych zagadnień dotyczących kryptografii.	
16. Cel przedmiotu: Celem przedmiotu jest prezentacja ponadpodstawowych algorytmów kryptograficznych oraz ich zastosowania w różnych dziedzinach techniki.	

17. Efekty kształcenia:[1]

Nr	Opis efektu kształcenia	Metoda sprawdzenia efektu kształcenia	Forma prowadzenia zajęć	Odniesienie do efektów dla kierunku studiów
1	Zna metody i techniki z zakresu ochrony danych dotyczące systemów komputerowych, systemów operacyjnych, sieci komputerowych.	Program komputerowy	Wykład, laboratorium	K_W03, K_W10

[1] należy wskazać ok. 5 – 8 efektów kształcenia

2	Potrafi korzystać z dokumentacji technicznej dotyczącej algorytmów kryptograficznych	Program komputerowy	Laboratorium	KW_06
3	Potrafi korzystać z gotowych implementacji algorytmów kryptograficznych uwzględniając specyfikę zadania	Program komputerowy	Laboratorium	K_U15, K_U17
4	Zna rozszerzone metody szyfrowania danych	Program komputerowy	Wykład, laboratorium	K_W10
5	Potrafi korzystać z narzędzi do obsługi urządzeń służących do uwierzytelniania użytkowników	Program komputerowy	Laboratorium	K_U13

18. Formy zajęć dydaktycznych i ich wymiar (liczba godzin)

W. 15 **Ćw.** **L.** **30** **P.** **Sem.**

19. Treści kształcenia:

Tematyka wykładów

Wprowadzenie. Efektywna implementacja: arytmetyka liczb całkowitych, arytmetyka modularna, potęgowanie modularne, Arytmetyka ciał skończonych. Ciała charakterystyki 2. Arytmetyka krzywych eliptycznych. Protokoły kryptograficzne wykorzystujące krzywe eliptyczne. Schematy podpisu. Szyfrowanie z kluczem publicznym. Uzgadnianie klucza. Bezpieczna implementacja. Ochrona przed atakami wykorzystującymi kanał boczny: analiza różnicowa mocy, analiza promieniowania EM, atak z wykorzystaniem pomiaru czasu wykonywania instrukcji. Realizacja mechanizmów kryptograficznych z wykorzystaniem niezaufanych systemów. Anonimowość w sieci. Anonimowość oparta na pseudonimach. Grupowe, ślepe podpisy. Systemy e-głosowania. Algorytmy kryptograficzne dedykowane dla urządzeń o ograniczonych zasobach systemowych. Karty inteligentne, tagi RFID.

Tematyka laboratorium:

Szyfrowanie plików
Wydajność algorytmów kryptograficznych
Kody uwierzytelniające wiadomości
Uwierzytelnianie użytkowników
Karty kryptograficzne
Steganografia

20. Egzamin: nie

21. Literatura podstawowa:

A. J. Menezes, P. C. Van Oorschot, S.A. Vanstone: Kryptografia stosowana.WNT

22. Literatura uzupełniająca:

M. Welschenbach: Kryptografia w C i C++. MIKOM

D. Hook: Kryptografia w Javie. Od podstaw. HELION

N. Koblitz: Algebraiczne aspekty kryptografii. WNT

B. Schneier: Kryptografia dla praktyków. WNT

23. Nakład pracy studenta potrzebny do osiągnięcia efektów kształcenia

Lp.	Forma zajęć	Liczba godzin kontaktowych / pracy studenta
1	Wykład	15/15
2	Ćwiczenia	/
3	Laboratorium	30/30
4	Projekt	/
5	Seminarium	/
6	Inne	/
	Suma godzin	/

24. Suma wszystkich godzin: 90

25. Liczba punktów ECTS:[2] **3**

26. Liczba punktów ECTS uzyskanych na zajęciach z bezpośrednim udziałem nauczyciela akademickiego 1

27. Liczba punktów ECTS uzyskanych na zajęciach o charakterze praktycznym (laboratoria, projekty) 2

26. Uwagi:

Zatwierdzono:

…….
(data i podpis prowadzącego)

……
(*data i podpis dyrektora instytutu/kierownika katedry/ Dyrektora Kolegium Języków Obcych/kierownika lub dyrektora jednostki międzywydziałowej)*

[2] 1 punkt ECTS – 30 godzin.