

KARTA PRZEDMIOTU

Kod przedmiotu		
Nazwa przedmiotu w języku	polskim	Szyfrowanie i bezpieczeństwo danych
	angielskim	Data encryption and security

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	Elektronika i Telekomunikacja
1.2. Forma studiów	studia niestacjonarne
1.3. Poziom studiów	studia I- stopnia inżynierskie
1.4. Profil studiów	praktyczny
1.6. Osoba przygotowująca kartę przedmiotu	dr inż. Tomasz Ruść
1.7. Kontakt	t.rusc@wstkt.pl

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Język wykładowy	polski
2.2. Wymagania wstępne	Algebra wyższa, Probabilistyka i statystyka

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Formy zajęć	Wykład, laboratorium, projekt	
3.2. Miejsce realizacji zajęć	Stacjonarne: Zajęcia w pomieszczeniu dydaktycznym WSTKT – Pracownia Komputerowa Zdalne: Spotkania zespołu Aplikacja Teams Wymagan indywidualnie od słuchaczy komputera z możliwością instalacji oprogramowania wskazanego przez prowadzącego	
3.3. Forma zaliczenia zajęć	wykłady – egzamin, ćwiczenia laboratoryjne – zaliczenie z oceną projekt – zaliczenie z oceną	
3.4. Metody dydaktyczne	Wykład - wykład z prezentacją multimedialną Laboratorium - ćwiczenia laboratoryjne Projekt – zadanie projektowe do samodzielnego wykonania	
3.5. Wykaz literatury	podstawowa	1. Wobst R. : „Kryptologia. Budowa i łamanie zabezpieczeń”, Wydawnictwo RM 2001 2. Friedrich L. B.: „Sekrety Kryptografii”, Wydawnictwo Helion 2002 3. Stinson D. R.: "Kryptografia w teorii i w praktyce", WNT 1995
	uzupełniająca	

4. CELE, TREŚCI I EFEKTY UCZENIA SIĘ

4.1. Cele przedmiotu:

Wykład:

C1. Poznanie metod szyfrowania danych i zapewnienia bezpieczeństwa systemów informatycznych

Ćwiczenia laboratoryjne, projekt:

C1. Praktyczne sprawdzenie działania szyfrów w programie CrypTool wyk

4.2. TREŚCI PROGRAMOWE:

Wykład:

Rola i znaczenie procesorów sygnałowych, ze szczególnym uwzględnieniem ich zastosowań w telekomunikacji
Architektura wybranych procesorów sygnałowych serii DaVinci firmy Texas Instruments Inc. – podsystem ARM
Architektura wybranych procesorów sygnałowych serii DaVinci firmy Texas Instruments Inc. – podsystem DSP
Arytmetyka stałopozycyjna i zmiennopozycyjna Transformaty FFT i IFFT i ich przykładowe implementacje
Standard JPEG w zagadnieniach kompresji obrazów – przykładowe implementacje Wybrane kodeki audio i ich przykładowe zastosowania w przetwarzaniu dźwięku.

Laboratorium:

1. Klasyczne algorytmy szyfrowania
2. Przeprowadzenie kryptoanalizy dla klasycznych algorytmów szyfrowania
3. Blokowe algorytmy szyfrowania.
4. Asymetryczne algorytmy szyfrowania.
5. Podpis elektroniczny.
6. Kryptoanaliza algorytmów symetrycznych i asymetrycznych.

Projekt:

W ramach zajęć projektowych student ma wykonać programowe implementacje (tj. utworzyć projekt, przesymulować i zweryfikować poprawność kodu oraz uruchomić i zaprezentować jego działanie na systemie rozwojowym DSP) wybranych algorytmów przetwarzania obrazów lub sygnałów audio i wideo na procesorach serii DaVinci firmy Texas Instruments Inc. Dodatkowo student ma opracować i przedstawić dokumentację techniczną projektu, obejmującą szczegóły programowej implementacji oraz elementy architektury wykorzystywanego w projekcie systemu DSP.

4.3 Przedmiotowe efekty uczenia się

Efekt	Student, który zaliczył przedmiot	Odniesienie do efektów kształcenia
W zakresie WIEDZY		
W01	Zna wybrane algorytmy szyfrowania i systemy bezpieczeństwa oparte na nich.	EIT1A_W01
W02	Posiada wiedzę w zakresie zapewnienia bezpieczeństwa dostępu, transmisji oraz przechowywania informacji.	EIT1A_W12
W03	Ma uporządkowaną, wiedzę obejmującą zagadnienia tworzenia podpisu cyfrowego.	EIT1A_W01
w zakresie UMIEJĘTNOŚCI:		
U01	Potrafi samodzielnie właściwie dobierać elementy bezpieczeństwa komputerowego do postawionych zadań..	EIT1A_U14
U02	Potrafi posługiwać się podstawowymi pojęciami z zakresu bezpieczeństwa i szyfrowania danych	EIT1A_U05

w zakresie **KOMPETENCJI SPOŁECZNYCH:**

K01	Dąży do ciągłego podnoszenia kompetencji zawodowych	EiT1A_K01
K02	Rozumie pozatechniczne i społeczne aspekty praktycznego stosowania zdobytej wiedzy i umiejętności oraz związaną z tym odpowiedzialność	EiT1A_K04
K03	ma świadomość roli inżyniera w przekazywaniu społeczeństwu kompetentnych informacji dotyczących szyfrowania i zabezpieczania danych	EiT1A_K06

4.4. Sposoby weryfikacji osiągnięcia przedmiotowych efektów uczenia się									
Efekty przedmiotowe (symbol)	Sposób weryfikacji (+/-)								
	Kolokwium			Zadania domowe			Sprawozdania		
	Forma zajęć			Forma zajęć			Forma zajęć		
	W	L	P	W	L	P	W	L	P
W01	+								
W02	+								
W03	+								
U01								+	
U02								+	
K01									+
K02									+
K03									+

4.5. Kryteria oceny stopnia osiągnięcia efektów uczenia się		
Forma zajęć	Ocena	Kryterium oceny
Wykład (W)	3	osiągnięcie <50-60) % wymogów stosowanych w metodach oceny
	3,5	osiągnięcie <61-70) % wymogów stosowanych w metodach oceny
	4	osiągnięcie <71-80) % wymogów stosowanych w metodach oceny
	4,5	osiągnięcie <81-90) % wymogów stosowanych w metodach oceny
	5	osiągnięcie <91-100> % wymogów stosowanych w metodach oceny
Laboratorium (L)	3	osiągnięcie <50-60) % wymogów stosowanych w metodach oceny
	3,5	osiągnięcie <61-70) % wymogów stosowanych w metodach oceny
	4	osiągnięcie <71-80) % wymogów stosowanych w metodach oceny
	4,5	osiągnięcie <81-90) % wymogów stosowanych w metodach oceny
	5	osiągnięcie <91-100> % wymogów stosowanych w metodach oceny
Projekt (P)	3	osiągnięcie <50-60) % wymogów stosowanych w metodach oceny
	3,5	osiągnięcie <61-70) % wymogów stosowanych w metodach oceny
	4	osiągnięcie <71-80) % wymogów stosowanych w metodach oceny
	4,5	osiągnięcie <81-90) % wymogów stosowanych w metodach oceny
	5	osiągnięcie <91-100> % wymogów stosowanych w metodach oceny

5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
	Studia niestacjonarne
<i>LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/</i>	
<i>Udział w wykładach*</i>	15
<i>Udział w ćwiczeniach, konwersatoriach, laboratoriach*</i>	15
<i>Udział w konsultacjach</i>	
<i>Udział w egzaminie/kolokwium zaliczeniowym*</i>	1
<i>SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/</i>	
<i>Przygotowanie do wykładu, zaliczenia z wykładu*</i>	24
<i>Przygotowanie do ćwiczeń, konwersatorium, laboratorium*</i>	35
<i>Przygotowanie do egzaminu/kolokwium*</i>	
<i>Zebranie materiałów do projektu, kwerenda internetowa, opracowanie projektu*</i>	60
<i>Opracowanie prezentacji multimedialnej*</i>	
<i>Inne (należy wskazać jakie? np. e-learning pod kontrolą nauczyciela)*</i>	
ŁĄCZNA LICZBA GODZIN	150
PUNKTY ECTS za przedmiot	6

**niepotrzebne usunąć*

Przyjmuję do realizacji (data i czytelne podpisy osób prowadzących przedmiot w danym roku akademickim)

.....