KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Kryptografia i bezpieczeństwo sprzętowe w inżynierii komput.	**1010542321010510177**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**ogólnoakademicki**	**1 / 2**

Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
Mikrosystemy informatyczne	**polski**	**obligatoryjny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
II stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **15** Ćwiczenia: **-** Laboratoria: **-** Projekty/seminaria: **30**	**4**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny)	(ogólnouczelniany, z innego kierunku)
kierunkowy	**z danego kierunku**

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**4 100%**
nauki techniczne	**4 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Michał Melosik
email: michal.melosik@put.poznan.pl
tel. 61 6652504
Katedra Inżynierii Komputerowej
ul. Piotrowo 3a, 61-138 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu podstaw nieprzeważania sygnałów, języku opisu sprzętu VHDL oraz VHDL-AMS, elektroniki oraz podstaw programowania. . Student powinien wykazywać się znajomością środowisk Matlab/SciLab/Octave/R.
2	**Umiejętności:**	Powinien posiadać umiejętność rozwiązywania podstawowych problemów z zakresu projektowania i analizowana układów cyfrowych oraz analogowych. Student powinien posiadać umiejętności szukania potrzebnych informacji we wskazanych źródłach. Student powinien wykazywać umiejętności wyciągania wniosków oraz kształtowania oceny prezentowanych rozwiązań.
3	**Kompetencje społeczne**	Dodatkowo student powinien również rozumieć konieczność poszerzania swoich kompetencji oraz powinien być gotowy do współpracy w ramach zespołu. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu:

- Zaznajomienie studentów z podstawowymi zagadnieniami kryptografii i bezpieczeństwa sprzętowego w inżynierii komputerowej.
- Przekazanie studentom podstawowej wiedzy w zakresie struktury wybranych układów kryptograficznych.
- Umiejętność tworzenia i adaptacji w warstwie sprzętowej systemów wbudowanych wybranych modułów kryptograficznych
- Rozwijanie u studentów umiejętności rozwiązywania problemów zastosowania optymalnego i właściwego doboru platformy sprzętowej oraz IPCorów.
- Kształtowanie u studentów umiejętności pracy zespołowej poprzez realizacje elementów projektu i połączenie ich w całość.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Ma zaawansowaną wiedzę szczegółową z zakresu projektowania systemów informatycznych, systemów wbudowanych, układów elektronicznych - [K2st_W3]
2. Ma zaawansowaną i szczegółową wiedzę o procesach z pogranicza informatyki i elektroniki zachodzących w cyklu życia wbudowanych systemów bezpieczeństwa i kryptografii - [K2st_W5]
3. Zna zaawansowane metody i techniki stosowane w projektowaniu i weryfikacji sprzętowych systemów bezpieczeństwa - [K2st_W6]
4. Ma wiedzę nt. kodeksów etycznych związanych z pracą naukowo-badawczą w zakresie bezpieczeństwa sprzętowego w inżynierii komputerowej - [K2st_W7]

Umiejętności:

1. Potrafi interdyscyplinarnie łączyć wybrane zagadnienia z elektroniki, fizyki z wiedzą z różnych obszarów informatyk - [K2st_U5]

2. Potrafi ocenić przydatność nowych metod w projektowaniu sprzętowych systemów bezpieczeństwa oraz wykorzystać najnowsze metod do ich testowania - [K2st_U6]

3. Potrafi dostrzec ograniczenia metod i narzędzi stosowanych w projektowaniu sprzętowych systemów kryptograficznych w kontekście bezpieczeństwa sprzętowego - [K2st_U9]

4. Potrafi stosując nowe metody rozwiązać złożone problemy z zakresu wykrywania zagrożeń w kryptografii sprzętowej i sprzętowym bezpieczeństwie danych - [K2st_U10]

Kompetencje społeczne:

1. Rozumie, że w informatyce, a w szczególności w projektowaniu sprzętowych systemów kryptograficznych wiedza i umiejętności szybko stają się przestarzałe - [K2st_K1]

2. Rozumie znaczenie wykorzystania najnowszych osiągnięć informatycznych w rozwiązywaniu problemów badawczych nad poprawą bezpieczeństwa sprzętowego - [K2st_K2]

Sposoby sprawdzenia efektów kształcenia

Ocena formująca:

- w zakresie wykładów: na podstawie odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach,
- w zakresie projektów / ćwiczeń: na podstawie oceny bieżącego postępu realizacji zadań oraz końcowej oceny projektu,

Ocena podsumowująca:

- w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez przeprowadzenie egzaminu pisemnego i ustnego
- w zakresie projektów/laboratoriów weryfikowanie założonych efektów kształcenia realizowane jest przez ocenę z postępu realizacji zadnia projektowego, ocenianie ciągłe, na każdych zajęciach (odpowiedzi ustne) ? premiowanie przyrostu umiejętności posługiwania się poznanymi zasadami i metodami, ocena poziomu zaawansowania realizacji projektu. Dodatkowo również przez ocenę dokumentacji tworzonej systematycznie wraz z postępami prac projektowych; dokumentacja przygotowywana częściowo w trakcie zajęć, a częściowo po ich zakończeniu; ocena ta obejmuje także umiejętność pracy w zespole.

Uzyskiwanie punktów dodatkowych za aktywność podczas zajęć, a szczególnie za:

- omówienia dodatkowych aspektów zagadnienia,
- efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,
- umiejętność współpracy w ramach zespołu praktycznie realizującego zadanie szczegółowe w laboratorium,
- uwagi związane z udoskonaleniem materiałów dydaktycznych,
- wskazywanie trudności percepcyjnych studentów umożliwiające bieżące doskonalenia procesu dydaktycznego.

Treści programowe

W zakresie wykładów omawiane zostaną następujące zagadnienia:

- generatory losowe TRBG, PRBG, CSPRBG i ich zastosowania bezpieczeństwie sprzętowym systemów wbudowanych oraz inżynierii komputerowej
- wybrane algorytmy kryptograficzne
- tryby szyfrowania
- proces projektowania systemu kryptograficznego, wymogi bezpieczeństwa, narzędzia weryfikacyjne
- generator liczb losowych i generatory binarnych sekwencji losowych ich zastosowanie w kryptografii
- alternatywne metody kryptograficzne na przykładzie kryptografii chaotycznej
- zagadnienia związane z zastosowaniem unikalnych funkcji sprzętowych PUF w szyfrowaniu oraz identyfikacji i autoryzacji systemów mikroelektronicznych. Rodzaje PUF, sposoby ich implementacji oraz praktyczne zastosowania.
- bezpieczeństwo sprzętowe PCB, ataki sprzętowe dokonywane na poziomie PCB
- problematyka trojanów sprzętowych w systemach wbudowanych. Klasyfikacja trojanów sprzętowych, zasada działania, metody wykrywania trojanów sprzętowych oraz sposoby zabezpieczenia przed ingerencja w system wbudowany
- tendencje rozwojowe we współczesnej kryptografii, nowe kierunki rozwoju: kryptografia chaotyczna, kwantowe generatory losowe

Zajęcia projektowe obejmują realizację projektów związanych:

-praktyczną realizacją wybranych modułów sprzętowych / programowo-sprzętowych / programowych dla istotnych w bezpieczeństwie sprzętowym inżynierii komputerowej.

Metody dydaktyczne:

-wykład: prezentacja multimedialna, wykład tradycyjny, prezentacja ilustrowana przykładami podawanymi na tablicy,

-zajęcia projektowe: realizacja projektu zgodnie z wytycznymi, dyskusja, praca w zespole

Literatura podstawowa:

1. A. Chrzęszczyk, Algorytmy teorii liczb i kryptografii w przykładach, wyd. BTC, 2010
2. M. Karbowski, Podstawy kryptografii., wyd. Helion, 2006
3. A. J. Menezs, Kryptografia stosowana, wyd. WNT, 2005
4. C. Parr, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010

Literatura uzupełniająca:

1. M. Melosik, W. Marszalek, "Using the 0-1 test for chaos to detect hardware trojans in chaotic bit generators", Electronics Letters 52 (11), 919-921
2. M. Melosik, P. Sniatala, W. Marszalek, "Hardware Trojans detection in chaos-based cryptography", Bulletin of the Polish Academy of Sciences Technical Sciences, 65 (5), 725-732 2017

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. udział w zajęciach laboratoryjnych / ćwiczeniach	30
2. przygotowanie do ćwiczeń laboratoryjnych	10
3. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych.	2
4. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych / projektu (częściowo realizowane drogą elektroniczną)	2
5. napisanie programu / programów, uruchomienie I weryfikacja (czas poza zajęciami laboratoryjnymi)	16
6. przygotowanie do egzaminu I obecność na egzaminie	10
7. udział w wykładach	15
8. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 150 stron	15

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	100	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	47	2
Zajęcia o charakterze praktycznym	48	2