KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Kryptografia i bezpieczeństwo sprzętowe w inżynierii komputerowej

Przedmiot

Kierunek studiów

Informatyka

Studia w zakresie (specjalność)

Mikrosystemy informatyczne

Poziom studiów

drugiego stopnia

Forma studiów

stacjonarne

Rok/semestr

1/2

Profil studiów

ogólnoakademicki

Język oferowanego przedmiotu

Polski

Wymagalność

obligatoryjny

Liczba godzin

Wykład

15

Laboratoria

Inne (np. online)

Ćwiczenia

Projekty/seminaria

30

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

Dr inż. Michał Melosik

email: michal.melosik@put.poznan.pl

wydział: Informatyki i Telekomunikacji

adres: Piotrowo 3A 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student powinien posiadać podstawową wiedzę z zakresu podstaw przetwarzania sygnałów, elektroniki,

języku opisu sprzętu VHDL oraz VHDL-AMS, podstaw programowania. 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. 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

1. Zaznajomienie studentów z podstawowymi zagadnieniami kryptografii i bezpieczeństwa sprzętowego w inżynierii komputerowej.

2. Przekazanie studentom podstawowej wiedzy w zakresie struktury wybranych układów kryptograficznych.

3. Rozwijanie umiejętności tworzenia i adaptacji w warstwie sprzętowej systemów wbudowanych wybranych modułów kryptograficznych

4. Rozwijanie u studentów umiejętności doboru optymalnej platformy sprzętowej oraz IPCorów.

5. Kształtowanie u studentów umiejętności pracy zespołowej poprzez realizacje elementów projektu i połączenie ich w całość.

Przedmiotowe efekty uczenia się

Wiedza
ma zaawansowaną wiedzę szczegółową z zakresu projektowania systemów informatycznych, systemów wbudowanych, układów elektronicznych; ma zaawansowaną i szczegółową wiedzę o procesach z pogranicza informatyki i elektroniki zachodzących w cyklu życia wbudowanych systemów bezpieczeństwa i kryptografii; zna zaawansowane metody i techniki stosowane w projektowaniu i weryfikacji sprzętowych systemów bezpieczeństwa; ma wiedzę nt. kodeksów etycznych związanych z pracą naukowo-badawczą w zakresie bezpieczeństwa sprzętowego w inżynierii komputerowej.

Umiejętności
potrafi interdyscyplinarnie łączyć wybrane zagadnienia z elektroniki, fizyki z wiedzą z różnych obszarów informatyk; potrafi ocenić przydatność nowych metod w projektowaniu sprzętowych systemów bezpieczeństwa oraz wykorzystać najnowsze metod do ich testowania; potrafi dostrzec ograniczenia metod i narzędzi stosowanych w projektowaniu sprzętowych systemów kryptograficznych w kontekście bezpieczeństwa sprzętowego; potrafi stosując nowe metody rozwiązać złożone problemy z zakresu wykrywania zagrożeń w kryptografii sprzętowej i sprzętowym bezpieczeństwie danych.

Kompetencje społeczne
rozumie, że w informatyce, a w szczególności w projektowaniu sprzętowych systemów

kryptograficznych wiedza i umiejętności szybko stają się przestarzałe; rozumie znaczenie wykorzystania najnowszych osiągnięć informatycznych w rozwiązywaniu problemów badawczych nad poprawą bezpieczeństwa sprzętowego.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
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 lub ustnego

- w zakresie projektów/laboratoriów weryfikowanie założonych efektów kształcenia realizowane jest przez ocenę z postępu realizacji zadnia projektowego, ocenianie ciągłe, premiowanie przyrostu umiejętności posługiwania się poznanymi zasadami i metodami, ocena poziomu zaawansowania realizacji projektu. Ocena przygotowanej dokumentacji/raportu.

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.

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, alternatywne metody kryptograficzne na przykładzie kryptografii chaotycznej

- PUF w mikroelektronice

- bezpieczeństwo sprzętowe PCB, ataki sprzętowe dokonywane na poziomie PCB

- Trojany sprzętowe

- kierunki rozwoju współczesnej kryptografii (kwantowe generatory losowe)

Zajęcia projektowe obejmują realizację projektów związanych:

- praktyczną implementacją wybranych modułów sprzętowych, programowo-sprzętowych, programowych.

Metody dydaktyczne

wykład: prezentacja multimedialna, wykład tradycyjny,

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

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

	Godzin	ECTS
Łączny nakład pracy	100	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2
Praca własna studenta (studia literaturowe, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)[1]	55	2

1 niepotrzebne skreślić lub dopisać inne czynności