

KARTA OPISU MODUŁU KSZTAŁCENIA		
Nazwa modułu/przedmiotu Kryptografia i bezpieczeństwo sprzętowe w inżynierii komput.		Kod 1010542321010510177
Kierunek studiów Informatyka	Profil kształcenia (ogólnoakademicki, praktyczny) ogólnoakademicki	Rok / Semestr 1 / 2
Ścieżka obieralności/specjalność Mikrosystemy informatyczne	Przedmiot oferowany w języku: polski	Kurs (obligatoryjny/obieralny) obligatoryjny
Stopień studiów: II stopień	Forma studiów (stacjonarna/niestacjonarna) stacjonarna	
Godziny Wykłady: 15 Ćwiczenia: - Laboratoria: - Projekty/seminaria: 30		Liczba punktów 4
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) inny		(ogólnouczeniowy, z innego kierunku) ogólnouczeniowy
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki		Podział ECTS (liczba i %)
Odpowiedzialny za przedmiot / wykładowca: mgr 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 nieprzewodzenia 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 analizowania 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 we współczesnej kryptografii. - Przekazanie studentom podstawowej wiedzy w zakresie realizacji wybranych algorytmów kryptograficznych a w szczególności ich sprzętowej realizacji. - Umiejętność tworzenia systemów zabezpieczenia i autoryzacji we współczesnych systemach wbudowanych. - Rozwijanie u studentów umiejętności rozwiązywania problemów zastosowania optymalnego i właściwego doboru algorytmu kryptograficznego. - Kształtowanie u studentów umiejętności pracy zespołowej poprzez realizację elementów projektu i połączenie ich w całość.		
Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia		
Wiedza: 1. ma podbudowaną teoretycznie szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki - [K_W5] 2. ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce i w wybranych pokrewnych dyscyplinach naukowych - [K_W6] 3. ma podstawową wiedzę o cyklu życia systemów informatycznych sprzętowych lub programowych - [K_W7] 4. zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu prostych zadań informatycznych z zakresu budowy układów cyfrowych, w tym systemów komputerowych, systemów wbudowanych - [K_W8]		
Umiejętności:		

1. potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł (w języku ojczystym i angielskim), integrować je, dokonywać ich interpretacji i krytycznej oceny, wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie - [K_U1]
2. potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia - [K_U5]
3. potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych metody analityczne, symulacyjne oraz eksperymentalne - [K_U9]
4. potrafi - przy formułowaniu i rozwiązywaniu zadań inżynierskich - integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne - [K_U10]
5. potrafi formułować i testować hipotezy związane z problemami inżynierskimi i prostymi problemami badawczymi - [K_U12]
6. potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych - [K_U13]
Kompetencje społeczne:
1. rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe - [K_K1]
2. zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych lub też do poważnej utraty zdrowia, a nawet życia - [K_K4]
3. potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania - [K_K6]

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 zadania projektowego, ocenianie ciągle, 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

- wprowadzenie do kryptografii, zarys historyczny sposobów zabezpieczania danych oraz autoryzacji. Zagadnienia związane z kryptografią symetryczną oraz asymetryczną. Budowa zasady działania oraz implementacja wybranych algorytmów symetrycznych i asymetrycznych. - tryby szyfrowania oraz ich docelowe przeznaczenie. - proces projektowania całego systemu kryptograficznego, wymogi bezpieczeństwa, narzędzia weryfikacyjne. - generator liczb losowych i generatory binarnych sekwencji losowych ich zastosowanie w kryptografii. Implementacja i realizacja wybranych generatorów binarnych sekwencji losowych w systemach wbudowanych - zagadnienia związane z zastosowaniem unikalnych funkcji sprzętowych PUF w szyfrowaniu oraz identyfikacji i autoryzacji systemów mikroelektronicznych. Rodzaje PUF, sposoby ich implementacji oraz praktyczne zastosowania. - problem trojanów sprzętowych w systemach wbudowanych. Klasyfikacja trojanów sprzętowych, zasada działania, metody wykrywania trojanów sprzętowych oraz sposoby zabezpieczenia przed ingerencją w system wbudowany - tendencje rozwojowe we współczesnej kryptografii, nowe kierunki rozwoju: kryptografia chaotyczna, kryptografia kwantowa																		
Zajęcia projektowe obejmują realizację projektów związanych: - Implementacją wybranych algorytmów kryptografii symetrycznej i asymetrycznej oraz trybów szyfrowania w środowisku Matlab/Scilab/Octave/R. - Implementacją wybranych generatorów sekwencji losowych na matrycach FPGA i FPAA. - Realizację systemów autoryzacji w systemach wbudowanych.																		
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:																		
Literatura uzupełniająca:																		
Bilans nakładu pracy przeciętnego studenta																		
<table><tr><th>Czynność</th><th>Czas (godz.)</th></tr><tr><td>1. udział w zajęciach laboratoryjnych / ćwiczeniach</td><td>45</td></tr><tr><td>2. przygotowanie do ćwiczeń laboratoryjnych</td><td>30</td></tr><tr><td>3. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych.</td><td>5</td></tr><tr><td>4. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych / projektu (częściowo realizowane drogą elektroniczną)</td><td>10</td></tr><tr><td>5. napisanie programu / programów, uruchomienie i weryfikacja (czas poza zajęciami laboratoryjnymi)</td><td>10</td></tr><tr><td>6. przygotowanie do egzaminu i obecność na egzaminie (8+2 godz.)</td><td>30</td></tr><tr><td>7. udział w wykładach</td><td>10</td></tr><tr><td>8. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 100 stron</td><td></td></tr></table>	Czynność	Czas (godz.)	1. udział w zajęciach laboratoryjnych / ćwiczeniach	45	2. przygotowanie do ćwiczeń laboratoryjnych	30	3. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych.	5	4. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych / projektu (częściowo realizowane drogą elektroniczną)	10	5. napisanie programu / programów, uruchomienie i weryfikacja (czas poza zajęciami laboratoryjnymi)	10	6. przygotowanie do egzaminu i obecność na egzaminie (8+2 godz.)	30	7. udział w wykładach	10	8. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 100 stron	
Czynność	Czas (godz.)																	
1. udział w zajęciach laboratoryjnych / ćwiczeniach	45																	
2. przygotowanie do ćwiczeń laboratoryjnych	30																	
3. dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych.	5																	
4. udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych / projektu (częściowo realizowane drogą elektroniczną)	10																	
5. napisanie programu / programów, uruchomienie i weryfikacja (czas poza zajęciami laboratoryjnymi)	10																	
6. przygotowanie do egzaminu i obecność na egzaminie (8+2 godz.)	30																	
7. udział w wykładach	10																	
8. zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi (10 stron tekstu naukowego = 1 godz.), 100 stron																		
Obciążenie pracą studenta																		
<table><tr><th>forma aktywności</th><th>godzin</th><th>ECTS</th></tr><tr><td>Łączny nakład pracy</td><td>150</td><td>6</td></tr><tr><td>Zajęcia wymagające bezpośredniego kontaktu z nauczycielem</td><td>87</td><td>3</td></tr><tr><td>Zajęcia o charakterze praktycznym</td><td>60</td><td>2</td></tr></table>	forma aktywności	godzin	ECTS	Łączny nakład pracy	150	6	Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	87	3	Zajęcia o charakterze praktycznym	60	2						
forma aktywności	godzin	ECTS																
Łączny nakład pracy	150	6																
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	87	3																
Zajęcia o charakterze praktycznym	60	2																