



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Kryptografia w systemach brzegowych [S2Inf1-PB>KRYPT]

Przedmiot

Kierunek studiów
Informatyka

Rok/Semestr
1/2

Studia w zakresie (specjalność)
Przetwarzanie brzegowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
30

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

5,00

Koordynatorzy

dr inż. Michał Melosik
michal.melosik@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student powinien posiadać podstawową wiedzę z zakresu podstaw przetwarzania sygnałów, podstaw programowania oraz 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. 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 w odniesieniu do technologii brzegowych i inżynierii komputerowej. 2. Przekazanie studentom podstawowej wiedzy w zakresie struktury wybranych rozwiązań kryptograficznych. 3. Rozwijanie umiejętności tworzenia i adaptacji w systemach brzegowych wybranych modułów kryptograficznych. 4. Rozwijanie u studentów umiejętności doboru optymalnych rozwiązań dla bezpieczeństwa systemów brzegowych 5. Kształtowanie u studentów umiejętności pracy zespołowej poprzez realizację elementów zadań i łączenia ich w całość.

Przedmiotowe efekty uczenia się

Wiedza:

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

Umiejętności:

potrafi interdyscyplinarnie łączyć wybrane zagadnienia z elektroniki, fizyki, statystyki, z wiedzą z różnych obszarów informatyk; potrafi ocenić przydatność nowych metod w projektowaniu zabezpieczeń dla systemów brzegowych oraz wykorzystać najnowsze metod do ich testowania; potrafi dostrzec ograniczenia metod i narzędzi stosowanych w projektowaniu systemów kryptograficznych w kontekście bezpieczeństwa sprzętowego i programowego; potrafi stosując nowe metody rozwiązać złożone problemy z zakresu wykrywania zagrożeń w sprzętowym i programowym bezpieczeństwie danych. informatycznych w rozwiązywaniu problemów badawczych nad poprawą bezpieczeństwa sprzętowego i programowego systemów brzegowych.

Kompetencje społeczne:

rozumie, że w informatyce, a w szczególności w projektowaniu systemów brzegowych wiedza i

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 laboratoriów / 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 danego zadania, ocenianie ciągle, premiowanie przyrostu umiejętności posługiwania się poznanymi zasadami i metodami, ocena poziomu zaawansowania w wykonywaniu zadań. Ocena przygotowanej dokumentacji/raportu z wykonanych zadań.

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 ramach laboratorium,
- uwagi związane z udoskonaleniem materiałów dydaktycznych.

Treści programowe

W ramach przedmiotu omawiane zostaną zagadnienia klasycznej kryptografii odnoszące się do specyfiki systemów przetwarzania brzegowego implementowanych w sposób sprzętowy lub programowo-sprzętowy.

Tematyka zajęć

1. Wprowadzenie do kryptografii.
2. Matematyczne podstawy kryptografii.
3. Losowość oraz generatory liczb losowych na przykładzie TRBG, PRBG, CSPRBG i ich zastosowania w bezpieczeństwie sprzętowym systemów wbudowanych oraz inżynierii komputerowej
4. Wybrane algorytmy kryptograficzne (symetryczne oraz asymetryczne), AES, RSA, alg. haszujące, EDSA, krzywe eliptyczne.
5. Protokoły wymiany klucza oraz protokoły kryptograficzne.
6. Standardy kryptograficzne.
7. Praktyczne aspekty kryptografii oraz socjotechniki w atakach na systemy bezpieczeństwa.
8. Typy ataków w kryptografii.

9. Wybrane zagadnienia z architektury bezpieczeństwa systemów mikro-informatycznych.
 10. Certyfikaty w kryptografii.
 11. Bezpieczeństwo sprzętowe w tym m.in. RoT, Chain of Trust, Secure boot, PUF, hardware Trojans, Threat Detecton Technolog
 12. Bezpieczeństwo ścieżki projektowania oraz łańcucha dostaw.
 13. Bezpieczeństwo, a kwestie etyczne oraz prawne.
- Zajęcia laboratoryjne obejmują realizację zadań dotyczących zagadnień aktualnie omawianych na wykładzie.

Metody dydaktyczne

Wykład: prezentacja multimedialna, wykład tradycyjny, dodatkowy materiał audio-wideo, specyfikacje techniczne, artykuły naukowe.

Zajęcia laboratoryjne: realizacja zadań zgodnie z wytycznymi, praca w zespole lub samodzielna, dyskusja problemowa.

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 | 125 | 5,00 |
| Zajęcia wymagające bezpośredniego kontaktu z nauczycielem | 60 | 2,50 |
| Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu) | 65 | 2,50 |