KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Podstawy kryptografii z zastosowaniami w telekomunikacji	**1010832131010802432**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Elektronika i Telekomunikacja	**ogólnoakademicki**	**2 / 3**

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

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

Godziny	Liczba punktów
Wykłady: **2** Ćwiczenia: **-** Laboratoria: **-** Projekty/seminaria: **1**	**3**

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

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**3 100%**
nauki techniczne	**3 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr hab. inż. Mieczysław Jessa
email: mjessa@et.put.poznan.pl
tel. +48 61 665 38 54
Wydział Elektroniki i Telekomunikacji
ul. Piotrowo 3A 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	K1_W01- Posiada usystematyzowaną wiedzę z zakresu analizy matematycznej, algebry i rachunku prawdopodobieństwa. K1_W14 (część) - Ma uporządkowaną wiedzę z podstaw radiokomunikacji, ma podstawową wiedzę w zakresie architektury i działania sieci mobilnych 2G, 3G i 4G. Ma podstawową wiedzę w zakresie architektury i działania bezprzewodowych sieci lokalnych i metod dostępu radiowego. K1_W22 (część) Ma uporządkowaną, podstawową wiedzę w zakresie struktury i funkcjonowania sieci telekomunikacyjnych. Ma podstawową wiedzę w zakresie podstaw, budowy i działania rozległych i lokalnych sieci komputerowych.
2	**Umiejętności:**	K1_U01 - Potrafi pozyskiwać informacje z literatury i baz danych oraz innych źródeł w języku polskim lub angielskim; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, wyciągać wnioski i uzasadniać opinie K1_U02 - Potrafi porozumiewać się w języku polskim lub angielskim w środowisk zawodowym i w innych środowiskach K1_U13 (część) - Potrafi się posługiwać językami programowania wysokiego poziomu C, C++, C#, potrafi pisać i uruchamiać programy dotyczące rozwiązywania i analizy różnych zagadnień elektroniki i telekomunikacji.
3	**Kompetencje społeczne**	K1_K01 - Zna ograniczenia własnej wiedzy i umiejętności, rozumie konieczność dalszego dokształcania się. K1_K02 - Posiada świadomość konieczności profesjonalnego podejścia do rozwiązywanych problemów technicznych i podejmowania odpowiedzialności za proponowane przez siebie rozwiązania techniczne. Potrafi realizować projekty zespołowe. K1_K04 - Potrafi formułować opinie na temat podstawowych wyzwań, przed którymi stoi współczesna elektronika i telekomunikacja. Posiada świadomość wpływu systemów i sieci telekomunikacyjnych i teleinformatycznych na kształtowanie społeczeństwa informacyjnego.

Cel przedmiotu:

Poznanie podstawowych pojęć kryptografii, zagrożeń charakterystycznych dla telekomunikacji przewodowej i bezprzewodowej oraz metod ich eliminacji. Poznanie i zrozumienie działania szyfrów blokowych, strumieniowych, kryptografii z kluczem tajnym i kryptografii z kluczem publicznym. Poznanie metod zapewniających tajność korespondencji, integralność danych, uwierzytelnienie nadawcy oraz niezaprzeczalność. Zapoznanie z różnymi rodzajami funkcjami skrótu oraz metodami podpisu cyfrowego. Poznanie podstawowych metod ataku na system kryptograficzny. Analiza bezpieczeństwa przykładowych systemów telekomunikacyjnych.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Ma praktyczną wiedzę na temat systemów bezpieczeństwa lub metod umożliwiających zapewnienie bezpieczeństwa informacji przesyłanych w sieciach telekomunikacyjnych. - [K2_W12]

Umiejętności:

1. Potrafi zastosować i/lub zaprojektować profesjonalne systemy nadzoru i bezpieczeństwa w różnego rodzaju sieciach bądź systemach telekomunikacyjnych. - [K2_U14]

Kompetencje społeczne:

1. Rozumie znaczenie społeczeństwa informacyjnego dla rozwoju kraju. - [K2_K02]
2. Ma poczucie odpowiedzialności za zaprojektowane systemy i zdaje sobie sprawę z zagrożeń dla ludzi i dla społeczeństwa w wypadku ich neiodpowiedzialnego zaprojektowania lub wykonania. - [K2_K06]

Sposoby sprawdzenia efektów kształcenia

-Egzamin pisemny.
-Raporty z wykonanych prac projektowych.
-Sprawdzanie aktywności podczas ćwiczeń projektowych.

Treści programowe

-Zagrożenia charakterystyczne dla telekomunikacji przewodowej i bezprzewodowej.
-System kryptograficzny ? terminologia. System z kluczem tajnym i z kluczem publicznym.
-Bezpieczeństwo systemu kryptograficznego.
-Szyfry blokowe i tryby użycia szyfrów blokowych.
-Szyfry strumieniowe ? właściwości i ograniczenia stosowania.
-Wybrane metody szyfrowania: szyfry jednoalfabetowe, wieloalfabetowe, szyfr Vigener?a, Enigma, DES, IDEA, AES.
-Wybrane metody szyfrowania z kluczem publicznym: szyfr ElGamala, RSA, szyfr Rabina.
-Kryptograficzna funkcja skrótu. Funkcje silnie i słabo bezkonfliktowe. Przykłady funkcji skrótu.
-Podpis cyfrowy.
-Podstawowe (ogólne) metody ataku na system kryptograficzny.
-Bezpieczeństwo przykładowych systemów telekomunikacyjnych (PDH, SDH, GSM, UMTS, 4G itp.)

Literatura podstawowa:

1. Kryptografia stosowana, A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, WNT, Warszawa 2005.
2. Kryptografia dla praktyków, B. Schneier, WNT, Warszawa, 2002.

Literatura uzupełniająca:

1. Kryptografia w praktyce, N. Ferguson, B. Schneier, Helion, 2004.
2. Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych, M. Kutyłowski, W-B. Strothmann, Read Me, Warszawa, 1999.
3. Wprowadzenie do kryptografii, J. A. Buchmann, PWN, Warszawa, 2006.

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Uczestniczenie w wykładach	30
2. Udział w ćwiczeniach projektowych	15
3. Samodzielne przygotowanie projektu na podstawie wiedzy pozyskanej na wykładzie	30
4. Przygotowanie do egzaminu	10
5. Udział w egzaminie	2
6. Konsultacje z wykładowcami	3

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	90	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	50	2
Zajęcia o charakterze praktycznym	25	1