Jednostka prowadząca: **Wydział Techniczny**

Kierunek studiów: **Elektronika i telekomunikacja**

Nazwa przedmiotu: **Kodowanie i kryptografia w telekomunikacji**

Charakter przedmiotu: kierunkowy, obowiązkowy

Typ studiów: inżynierskie I-go stopnia, stacjonarne/niestacjonarne

Formy dydaktyczne i terminarz:

Forma przedmiotu	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Rok studiów/Semestr	4/7		4/7		
Liczba godzin w semestrze	30/18		30/18		
Forma zaliczenia	zal.na ocenę		zal.na ocenę		
Liczba punktów ECTS	3/3		3/3		

WYKŁAD

Wymagania wstępne:
Brak wymagań wstępnych.

Cele kształcenia:
Zapoznanie studenta z ogólnymi problemami związanymi z transmisją danych. Przedstawienie sposobów kodowania informacji, wykrywania i korekcji błędów. Przekazanie podstawowej wiedzy z dziedziny ochrony przesyłanych danych oraz podstawowych systemów i algorytmów kryptograficznych wykorzystywanych w telekomunikacji.

Metody dydaktyczne:
Wykład aktywizujący z wykorzystaniem elementów metody problemowej i praktycznymi przykładami kodowania i szyfrowania informacji.

Zasady i kryteria zaliczenia:
Kolokwium zaliczeniowe z tematów 1-5 (kodowanie) oraz kolokwium zaliczeniowe z tematów 7-13 (kryptografia). Podstawą zaliczenia jest zdobycie co najmniej 50 % maksymalnej liczby punktów w dwu kolokwiach.

Treści programowe:
1. Elementy transmisji danych (system transmisji, kryteria jakości transmisji i jej optymalizacji, zakłócenia i błędy w kanałach telekomunikacyjnego, model binarnego kanału transmisji danych).
2. Charakterystyka kodów (metody kodowego zabezpieczenia przed błędami w transmisji, typy kodów korekcyjnych, struktura kodu blokowego, zdolność detekcyjna i korekcyjna kodu, pojęcie syndromu).
3. Kody liniowe (definicje kodu, kodowania i dekodowanie informacji, kody Hamminga).
4. Kody cykliczne (charakterystyka, generacja kodów cyklicznych, algorytm kodowania i dekodowania, realizacja techniczna).

5. Binarne kody cykliczne (cykliczne kody Hamminga).
6. Kolokwium z tematów 1-5.
7. Elementy kryptologii (ochrona danych, systemy i algorytmy kryptograficzne, kryptoanaliza).
8. Systemy kryptograficzne (klucz tajny, klucz jawny, ocena systemów).
9. Szyfry podstawieniowe i przestawieniowe.
10. Szyfry kaskadowe (charakterystyka szyfrów kaskadowych, algorytm Lucyfer, standard szyfrowania DES).
11. Klucze kryptograficzne (charakterystyka kluczy, generatory nieliniowe kluczy binarnych, zarządzanie kluczami).
12. Szyfry z kluczem jawnym (algorytmy z kluczem jawnym, algorytm Merklego-Hellmana, algorytm ElGamala, algorytm RSA).
13. Techniki szyfrowania i implementacje.
14. Kolokwium z tematów 7-13.

Literatura podstawowa:

1. Stinson D., *Kryptografia w teorii i praktyce*. WNT, Warszawa 2005.
2. Haykin S., *Systemy telekomunikacyjne*, t 2. WKŁ, Warszawa 2004.
3. Kutyłowski M., Strothmann Willy-B., *Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych.* Oficyna Wydawnicza READ ME, 1999.
4. Mochnacki W., *Kody korekcyjne i kryptografia*. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000. (Dolnośląska Biblioteka Cyfrowa www.dbc.wroc.pl).
5. Seidler J., *Systemy przesyłania informacji cyfrowych*. WNT, Warszawa 1976.

Literatura uzupełniająca:

1. Karbowski M., *Podstawy kryptografii*. Wydawnictwo HELION, Gliwice 2006.
2. Bauer F., *Sekrety kryptografii*. Wydawnictwo HELION, Gliwice 2002.
3. Schneier B., *Kryptografia dla praktyków*. WNT, Warszawa 2002.
4. Cormen T.H., Leiserson E., Rivest R.L., *Wprowadzenie do algorytmów*. WNT, Warszawa 1997.
5. Denning D.E.R., *Kryptografia i ochrona danych.* WNT, Warszawa 1992.

Efekty kształcenia:

Umiejętność określania roli kodowania w przesyłaniu informacji i kryteriów jakości transmisji, rozumienie i znajomość znaczenia i wykorzystania sposobów kodowania korekcyjnego przesyłanej informacji w kanałach transmisji danych oraz ich kryptograficznego zabezpieczenia, umiejętności ogólnego analizowanie przesyłanych informacji oraz oceny stanu zagrożenia ujawnienia przesyłanych kryptogramów.

Język wykładowy: polski.

LABORATORIUM

Wymagania wstępne:
Brak wymagań wstępnych.

Cele kształcenia:
Zapoznanie studentów z praktycznymi rozwiązaniami metod kodowania korekcyjnego i kryptografii.

Metody dydaktyczne:
Samodzielne przygotowanie się studentów i wykonanie ćwiczeń laboratoryjnych pod nadzorem wykładowcy.

Zasady i kryteria zaliczenia:
Pozytywna ocena z wszystkich ćwiczeń laboratoryjnych i wykonanych sprawozdań.

Treści programowe:
1. Zajęcia wprowadzające.
2. Operacje na pojedynczych bitach dowolnego bajta.
3. Zamiana tekstu na wartość binarną i odwrotnie.
4. Kodowanie informacji za pomocą liniowego kodu Hamminga (7,4).
5. Dekodowanie liniowego kodu Hamminga (7,4).
6. Kodowanie informacji za pomocą cyklicznego kodu Hamminga (7,4).
7. Dekodowanie wektora odebranego cyklicznego kodu Hamminga (7,4).
8. Szyfr Cezara.
9. Szyfr z dowolnym przesunięciem.
10. Szyfr przestawieniowy – macierz (kwadrat).
11. Szyfr XOR.
12. Szyfr Vigenere'a.
13. Szyfr Playfair.
14. Zajęcia rezerwowe (odróbcze).
15. Zaliczenie.

Literatura podstawowa:

1. Mochnacki W., *Kody korekcyjne i kryptografia*. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000. (Dolnośląska Biblioteka Cyfrowa www.dbc.wroc.pl).
2. Instrukcje laboratoryjne dla poszczególnych stanowisk, opracowanie dostępne w laboratorium „Kodowanie i kryptografia w telekomunikacji".

Literatura uzupełniająca:

1. Stinson D., *Kryptografia w teorii i praktyce*. WNT, Warszawa 2005.
2. Haykin S., *Systemy telekomunikacyjne*, t. 2. WKŁ, Warszawa 2004.

Efekty kształcenia:
Umiejętność kodowania przesyłanej kanałami transmisji danych informacji przy wykorzystaniu podstawowych kodów. Umiejętność szyfrowania przesyłanych informacji podstawowymi rodzajami szyfrów.

Osoby prowadzące:
dr inż. Mirosław Chrzanowski
mgr inż. Andrzej Rehlis