**Nazwa przedmiotu:**

Kryptografia i ochrona danych

**Koordynator przedmiotu:**

dr hab. Tomasz Adamski, prof. uczelni

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Fizyka Techniczna

**Grupa przedmiotów:**

Obowiązkowe

**Kod przedmiotu:**

1050-FTEDM-MSP-KOD

**Semestr nominalny:**

2 / rok ak. 2017/2018

**Liczba punktów ECTS:**

3

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

1. godziny kontaktowe – 46 h; w tym
a) obecność na wykładach – 30 h
b) obecność na ćwiczeniach– 15 h
c) obecność na egzaminie – 1 h
2. praca własna studenta – 29 h; w tym
a) przygotowanie do wykładów – 7 h
b przygotowanie do ćwiczeń– 15 h
c) przygotowanie do egzaminu – 7 h
Razem w semestrze 75 h, co odpowiada 3 pkt. ECTS

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

1. obecność na wykładach – 30 h
2. obecność na ćwiczeniach – 15 h
3. obecność na egzaminie – 1 h
Razem w semestrze 46 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

0

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład: | 450h |
| Ćwiczenia: | 225h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Probabilistyka, Algebra z geometrią, Podstawy i Zastosowania Teorii Informacji

**Limit liczby studentów:**

brak

**Cel przedmiotu:**

Wprowadzenie do metod kryptograficznych stosowanych w systemach komputerowych, sieciach komputerowych i sensorowych, rozproszonych systemach pomiarowych oraz w telekomunikacji.

**Treści kształcenia:**

Wykład:
1. Kryptografia - pojęcia podstawowe i szyfry klasyczne (2h)
2. Podstawy matematyczne kryptografii (4h)
3. Szyfry z kluczem publicznym (2h)
4. Szyfry z kluczem prywatnym (2h)
5. Generacja bitów, liczb losowych i pseudolosowych dla celów kryptograficznych (1h)
6. Algorytmy testowania pierwszości i generacja liczb pierwszych (2h)
7. Szyfry strumieniowe (2h)
8. Tryby wykorzystania szyfrów blokowych (1h)
9. Funkcje skrótu (2h)
10. Identyfikacja-uwierzytelnianie strony (2h)
11. Uwierzytelnianie dokumentu - podpisy cyfrowe (2h)
12. Efektywna implementacja algorytmów kryptograficznych (2h)
13. Uzgadnianie kluczy, dystrybucja kluczy, protokoły wymiany klucza (1h)
14. Dzielenie tajemnic (1h)
15. Protokoły kryptograficzne (1h)
16. Zarządzanie kluczami (key management), infrastruktura klucza publicznego (PKI) (1h)
17. Kryptografia kwantowa (2h)
Ćwiczenia:
1. Systemy kryptograficzne, szyfry klasyczne, ataki na szyfry klasyczne (2h)
2. Obliczanie wartości funkcji Eulera, tw. Eulera i jego zastosowania, pierścień i jego własności (1h)
3. Liczby pierwsze i testowanie pierwszości, sito Eratostenesa, algorytm Millera-Rabina (1h)
4. Grupy, podgrupy, dzielniki normalne, grupy ilorazowe, grupy cykliczne i ich własności, tw. Lagrange’a, logarytm dyskretny w grupie, krzywe eliptyczne, bazy Gaussa, bazy normalne (2h)
5. Pierścienie, ciała i ich własności, chińskie twierdzenie o resztach, zapis RNS, algorytmy konwersji z zapisu RNS na naturalny zapis binarny (2h)
6. Szyfry z kluczem publicznym (szyfr RSA, ElGamala, Rabina, NTRU), algorytm Diffiego-Hellmana uzgadniania kluczy (2h)
7. Szyfry z kluczem prywatnym (DES,AES,IDEA,TES, szyfry Feistala) (2h)
8. Algorytmy uwierzytalniania strony, jaskinia z wiedzą zerową, dowody z wiedzą zerową (1h)
9. Algorytmy uwierzytelnianie dokumentu, podpisy cyfrowe (podpisy ElGamala, podpis DSS) (1h)
10. Efektywne implementacje algorytmów kryptograficznych (algorytm Mongomery’ego, algorytm Barretta, szybkie podnoszenie do potęgi modulo) (1h)

**Metody oceny:**

Do uzyskania 200pkt: egzamin100 pkt, ćwiczenia 100 pkt (2 kolokwia + zadania domowe)
Do zaliczenia potrzeba min. 100 pkt

**Egzamin:**

tak

**Literatura:**

1. A.Menezes, P.van Oorsschot, S.Vanstone; Handbook of Applied Cryptography; CRC Press 1996.
2. N.Koblitz; Wykład z teorii liczb i kryptografii; WNT, Warszawa 1995.
3. N.Koblitz; Algebraiczne aspekty kryptografii; WNT, Warszawa 2000.
4. B.Schneier; Kryptografia dla praktyków; Wiley & WNT, Warszawa 1995.
5. J. Stokłosa, T.Bilski, T.Pankowski; Kryptograficzna ochrona danych w systemach komputerowych; PWN. Poznań 2001.
6. W.Stallings; Ochrona danych w sieci i intersieci; WNT, 1998.
7. T.Cormen, C.Leiserson, R.Rivest; Wprowadzenie do algorytmów; WNT, Warszawa 1997.
8. J.Pieprzyk, T.Hardjono,J.Seberry; Teoria bezpieczeństwa systemów komputerowych; Helion-Springer, Gliwice 2005.
9. T.Adamski, J,Ogrodzki; wprowadzenie do algorytmów komputerowych i struktur danych; Oficyna Wydawnicza PW 2014.
10. T.Adamski; Zbiór zadań z podstawy teoretycznych kryptografii i ochrony informacji; Oficyna Wydawnicza PW, 2014.

**Witryna www przedmiotu:**

brak

**Uwagi:**

brak

## Efekty przedmiotowe