**Nazwa przedmiotu:**

Wprowadzenie do współczesnej kryptologii

**Koordynator przedmiotu:**

Dr hab. inż. Konstanty Junosza-Szaniawski

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

1120-MAMNI-NSP-0111

**Semestr nominalny:**

1 / rok ak. 2022/2023

**Liczba punktów ECTS:**

4

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

1. godziny kontaktowe – 65 h; w tym
a) obecność na wykładach – 30 h
b) obecność na ćwiczeniach – 15 h
c) obecność na projekcie – 15 h
d) konsultacje – 5 h
2. praca własna studenta – 50 h; w tym
a) przygotowanie do ćwiczeń i do kolokwium – 20 h
a) przygotowanie i realizacja projektu – 25 h
b) zapoznanie się z literaturą – 5 h
Razem 115 h, co odpowiada 4 pkt. ECTS

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

a) obecność na wykładach – 30 h
b) obecność na ćwiczeniach – 15 h
b) obecność na projekcie – 15 h
d) konsultacje – 5 h
Razem 65 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

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

.

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

|  |  |
| --- | --- |
| Wykład: | 30h |
| Ćwiczenia: | 15h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Wymagania wstępne: Znajomość podstwowych pojęć dotyczących algorytmów, struktur danych, złożoności obliczeniowej, matematyki dyskretnej, algebry.

**Limit liczby studentów:**

Bez limitu

**Cel przedmiotu:**

Zapoznanie studentów z podstawami współczesnej kryptologii.

**Treści kształcenia:**

1. Systemy kryptograficzne. Podstawowe pojęcia kryptografii i kryptoanalizy.
2. Bezpieczeństwo kryptograficzne (oszacowanie, uzyskiwanie i dowodzenie bezpieczeństwa; rodzaje ataków):
a. Idealne szyfrowanie - szyfry z kluczem jednorazowym.
b. Generatory kluczy - podkreślenie znaczenia entropii.
3. Szyfrowanie kluczem prywatnym (symetryczne):
a. Tryby szyfrowania.
b. Szyfry blokowe: DES, AES (implementacje, bezpieczeństwo).
c. Szyfry strumieniowe.
4. Funkcje skrótu.
5. Szyfrowanie uwierzytelnione (algorytmy chroniące poufność i autentyczność), MAC.
6. Szyfrowanie kluczem publicznym (asymetryczne). Uzgodnienie klucza (Diffie-Hellman).
8. Podpis cyfrowy (RSA i DSA).
9. Zastosowanie krzywych eliptycznych.
10. Protokół SSL/TLS.
11. Protokoły kryptograficzne: inne i weryfikacja poprawności.
12. Kryptografia postkwantowa (informacyjnie: algorytm Shora; kryptografia na kratach).

**Metody oceny:**

Kolokwium, projekt

**Egzamin:**

nie

**Literatura:**

1. J-P. Aumasson, Nowoczesna kryptografia, PWN, Warszawa 2018.
2. J. Katz, Y. Lindell, Introduction to Modern Cryptography, Chapman and Hall/CRC, 2020.
3. N. Koblitz, Wykłady z teorii liczb i kryptografii, WNT, Warszawa 1995.
4. N. Koblitz, Algebraiczne aspekty kryptografii, WNT, Warszawa 1997.
5. N. Smart, Cryptography Made Simple, Springer International Publishing, 2016
6. L. Knudsen, M. Robshaw, The Block Cipher Companion, Springer-Verlag Berlin Heidelberg, 2011

**Witryna www przedmiotu:**

brak

**Uwagi:**

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka WWK\_W01:**

Ma wiedze o formalnych podstawach kryptologii i uwarunkowań modeli kryptologicznych

Weryfikacja:

Kolokwium,

**Powiązane charakterystyki kierunkowe:** M2\_W01, M2\_W02, M2\_W03, M2MCB\_W01, M2MCB\_W04, M2\_W04

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WWK\_W02:**

Ma wiedzę o aktualnych metodach oceny bezpieczeństwa algorytmów i protokołów kryptograficznych wykorzystujących modelowanie matematyczne.

Weryfikacja:

Kolokwium

**Powiązane charakterystyki kierunkowe:** M2\_W01, M2\_W02, M2\_W03, M2MCB\_W01, M2MCB\_W04, M2\_W04

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WWK\_W03:**

Ma wiedzę w zakresie zastosowania struktur algebraicznych w konstrukcji algorytmów i prokotołów kryptograficznych.

Weryfikacja:

Kolokwium

**Powiązane charakterystyki kierunkowe:** M2\_W02, M2\_W03, M2MCB\_W01, M2MCB\_W04, M2\_W04, M2\_W01

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WWK\_W04:**

Ma wiedzę o nowoczesnych kierunkach rozwoju kryptologii.

Weryfikacja:

Kolokwium

**Powiązane charakterystyki kierunkowe:** M2\_W03

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka WWK\_U01:**

Potrafi ocenić bezpieczeństwo podstawowych prymitywów kryptograficznych.

Weryfikacja:

Kolokwium, Sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U03, M2MCB\_U04

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WWK\_U02:**

Potrafi budować i stosować modele matematyczne w ocenie bezpieczeństwa algorytmów i protokołów kryptograficznych.

Weryfikacja:

Kolokwium, Sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U03, M2MCB\_U04

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka WWK\_K01:**

Rozumie przydatność i znaczenie nabytej wiedzy w obszarze bezpieczeństwa cyfrowego oraz jego znaczenie społeczne

Weryfikacja:

Sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_K02

**Powiązane charakterystyki obszarowe:**