

**"ZATWIERDZAM"**

.....

.....

**KARTA INFORMACYJNA PRZEDMIOTU**

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----------|-------------|---------------|-------------------------------------------------|-------------------|------|--|
| Nazwa przedmiotu                                        | Algorytmy strumieniowe                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                             |         |           |             |               |                                                 | Stream Algorithms |      |  |
| Kod przedmiotu                                          | WCYKWSM_AST.....AST                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Język wykładowy                                         | polski                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Profil studiów                                          | ogólnoakademicki                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Forma studiów                                           | studia stacjonarne                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Poziom studiów                                          | wojskowe studia jednolite magisterskie                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Rodzaj przedmiotu                                       | obowiązkowy                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Obowiązuje od naboru                                    | 2021/2022                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS | semestr                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | (x egzamin, + zaliczenie, # projekt)                                                                                                                                                                        |         |           |             |               |                                                 | punkty ECTS       |      |  |
|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | razem                                                                                                                                                                                                       | wykłady | ćwiczenia | laboratoria | projekt       | seminarium                                      |                   |      |  |
|                                                         | VII                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 44x                                                                                                                                                                                                         | 24      | 6         | 14+         |               |                                                 | 3.0               |      |  |
|                                                         | razem                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                             | 24      | 6         | 14          |               |                                                 | 3.0               |      |  |
| Przedmioty wprowadzające                                | ● Brak przedmiotów kształcenia wprowadzających                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Semestr/kierunek studiów                                | semestr 7 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Autor                                                   | mgr inż. Krzysztof Mańk                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Jednostka odpowiedzialna za przedmiot                   | WCY / IMK / LBK                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Skrócony opis przedmiotu                                | ● Wykład<br>● Ćwiczenia<br>● Laboratorium                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Pełny opis przedmiotu (treści programowe)               | lp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Semestr VII<br>temat/tematyka zajęć                                                                                                                                                                         |         |           |             | liczba godzin |                                                 |                   |      |  |
|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                             |         |           | wkł.        | ćw.           | lab.                                            | prj.              | sem. |  |
|                                                         | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Zasady szyfrowania strumieniowego. Różnice i podobieństwa do szyfrów blokowych. Tryby pracy szyfrów.                                                                                                        |         |           |             | 4             |                                                 |                   |      |  |
|                                                         | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Szyfry synchroniczne i samosynchronizujące się.                                                                                                                                                             |         |           |             | 2             |                                                 | 2                 |      |  |
|                                                         | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Liniowy rejestr przesuwający (LFSR) jako generator klucza. Okres i złożoność liniowa generatora.                                                                                                            |         |           |             | 4             | 2                                               | 2                 |      |  |
|                                                         | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Reguły konstruowania generatorów.                                                                                                                                                                           |         |           |             | 8             | 2                                               | 4                 |      |  |
|                                                         | 5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Przykłady generatorów, generatory wykorzystujące szyfry blokowe.                                                                                                                                            |         |           |             | 2             |                                                 | 2                 |      |  |
|                                                         | 6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Ocena jakości generatora. Testy losowości.                                                                                                                                                                  |         |           |             | 4             | 2                                               | 4                 |      |  |
|                                                         | Razem                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                             |         |           | 24          | 6             | 14                                              |                   |      |  |
| Literatura                                              | podstawowa:                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
|                                                         | ● Rueppel R. A., Analysis and Design of Stream Ciphers, 1986<br>● Rainer A. Rueppel, Stream Ciphers, rozdział 2 z Contemporary Cryptography G.J. Simmons<br>● Robling-Denning D. E., Kryptografia i ochrona danych, 1982<br>● Menezes A., van Oorschot P., Vanstone S., Handbook of Applied Cryptography<br>● Schneier B., Kryptografia dla praktyków, wyd. II, 2002<br>uzupełniająca:<br>● Szmidt J, Misztal M., Wstęp do kryptologii, 2003<br>● Golomb S.W., Shift register sequences |                                                                                                                                                                                                             |         |           |             |               |                                                 |                   |      |  |
| Efekty uczenia się                                      | Symbol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Efekty kształcenia                                                                                                                                                                                          |         |           |             |               | odniesienie do efektów kształcenia dla kierunku |                   |      |  |
|                                                         | W1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie programowania, algorytmów i struktur danych.                                                                                      |         |           |             |               | K_W22                                           |                   |      |  |
|                                                         | W2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Ma ogólną wiedzę dotyczącą metod i technik kryptograficznych oraz ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie matematycznych podstaw kryptologii, systemów kryptograficznych. |         |           |             |               | K_W22                                           |                   |      |  |
|                                                         | W3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Ma wiedzę na temat zasad szyfrowania strumieniowego, reguł konstruowania komponentów szyfrów strumieniowych.                                                                                                |         |           |             |               | K_U19 K_W22                                     |                   |      |  |
|                                                         | W4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Ma wiedzę o znanych szyfrach strumieniowych, zna wymagania stawiane współczesnym algorytmom strumieniowym.                                                                                                  |         |           |             |               | K_W23                                           |                   |      |  |
|                                                         | U1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Potrafi wykazać się praktycznymi umiejętnościami z zakresu podstaw informatyki takimi, jak: projektowanie efektywnych algorytmów, szacowanie złożoności algorytmów i budowa automatów skończonych.          |         |           |             |               | K_U19                                           |                   |      |  |

|                                                                                                             | Symbol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Efekty kształcenia                                                                                                                                                                                                                              | odniesienie do efektów kształcenia dla kierunku |
|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
|                                                                                                             | U2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Potrafi samodzielnie pozyskiwać informacje z literatury, zna dostępne zbiory prac z dziedziny kryptologii. Potrafi samodzielnie przyswoić nowe informacje i przedstawić wyciągnięte wnioski, a w razie potrzeby uzasadnić przedstawione opinie. | K_U19                                           |
| Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się) | <ul style="list-style-type: none"><li>• Moduł kształcenia zaliczany jest na podstawie sprawdzianu pisemnego i ocen uzyskanych w trakcie ćwiczeń i laboratoriów. Sprawdzian pisemny polega na rozwiązaniu przez studenta zadań problemowych, ocenianych w skali punktowej. Warunkiem koniecznym uzyskania zaliczenia jest uzyskanie pozytywnej oceny ze sprawdzianu pisemnego. Na ocenę końcową składają się w 80% ocena ze sprawdzianu pisemnego, w 20% średnia ocen uzyskanych w trakcie ćwiczeń i laboratoriów.</li><li>• Efekty W1, W2, W3 i U1 sprawdzane są: kolokwium pisemnym. Efekt W4 sprawdzany jest w trakcie odpowiedzi ustnych podczas ćwiczeń i laboratoriów.</li></ul> |                                                                                                                                                                                                                                                 |                                                 |
| Bilans ECTS (nakład pracy studenta)                                                                         | SEMESTR 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Aktywność                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Obciążenie studenta                                                                                                                                                                                                                             |                                                 |
|                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Liczba godzin                                                                                                                                                                                                                                   | Liczba ECTS                                     |
|                                                                                                             | Udział w wykładach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 24                                                                                                                                                                                                                                              | 1                                               |
|                                                                                                             | Udział w laboratoriach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 14                                                                                                                                                                                                                                              | 0.5                                             |
|                                                                                                             | Udział w ćwiczeniach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 6                                                                                                                                                                                                                                               | 0.5                                             |
|                                                                                                             | Udział w projektach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0                                                                                                                                                                                                                                               | 0                                               |
|                                                                                                             | Udział w seminariach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 0                                                                                                                                                                                                                                               | 0                                               |
|                                                                                                             | Samodzielne studiowanie tematyki wykładów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 24                                                                                                                                                                                                                                              | 0.5                                             |
|                                                                                                             | Samodzielne przygotowanie do laboratoriów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 28                                                                                                                                                                                                                                              | 0.5                                             |
|                                                                                                             | Samodzielne przygotowanie do ćwiczeń                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Samodzielna realizacja projektu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Samodzielne przygotowanie do seminariów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Udział w konsultacjach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Przygotowanie do egzaminu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Przygotowanie do zaliczenia                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Udział w egzaminie / kolokwium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                 |                                                 |
|                                                                                                             | Sumaryczne obciążenie pracą studenta                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 96                                                                                                                                                                                                                                              | 3                                               |
|                                                                                                             | Zajęcia z udziałem nauczycieli                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 44                                                                                                                                                                                                                                              | 2                                               |
|                                                                                                             | Zajęcia powiązane z działalnością naukową                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 96                                                                                                                                                                                                                                              | 3                                               |
| Zajęcia o charakterze praktycznym                                                                           | 48                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 1.5                                                                                                                                                                                                                                             |                                                 |

autor

kierownik jednostki organizacyjnej  
odpowiedzialnej za przedmiot

mgr inż. Krzysztof Mańk  
tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Kojdecki Marek  
tytuł, stopień naukowy, imię, NAZWISKO, podpis