

"ZATWIERDZAM"

## KARTA INFORMACYJNA PRZEDMIOTU

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----------|-------------|-------------------------------------------------|---------------|------------|
| Nazwa przedmiotu                                        | Teoria ciał skończonych                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                              |         |           |             |                                                 | Finite Fields |            |
| Kod przedmiotu                                          | WCYKSWSM_TCS.....TCS                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Język wykładowy                                         | polski                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Profil studiów                                          | ogólnoakademicki                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Forma studiów                                           | studia stacjonarne                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Poziom studiów                                          | wojskowe studia jednolite magisterskie                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Rodzaj przedmiotu                                       |                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| 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 |
|                                                         | VIII                                                                                                                                                                                                                                                                                                                                                                                                                | 30+                                                                                                                                                                                                          | 20      | 10+       |             |                                                 |               | 3.0        |
|                                                         | razem                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                              | 20      | 10        |             |                                                 |               | 3.0        |
| Przedmioty wprowadzające                                | ● Brak przedmiotów kształcenia wprowadzających                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Semestr/kierunek studiów                                | semestr 8 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Autor                                                   | dr Piotr Kacprzyk                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Jednostka odpowiedzialna za przedmiot                   | Instytut Matematyki i Kryptologii, Wydział Cybernetyki                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Skrócony opis przedmiotu                                | ● wykład z możliwym wykorzystaniem technik audiowizualnych; podanie zadań do samodzielnego rozwiązania i tematów do studiowania.<br>● ćwiczenia rachunkowe ułatwiające opanowanie, zrozumienie i usystematyzowanie wiedzy wyniesionej z wykładów i własnych studiów studentów oraz nabycie umiejętności rachunkowych; podanie zadań do samodzielnego rozwiązania i tematów do studiowania; pisemna praca kontrolna. |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Pełny opis przedmiotu (treści programowe)               | lp.                                                                                                                                                                                                                                                                                                                                                                                                                 | Semestr VIII<br>temat/tematyka zajęć                                                                                                                                                                         |         |           |             | liczba godzin                                   |               |            |
|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                     | wkl.                                                                                                                                                                                                         | ćw.     | lab.      | prj.        | sem.                                            |               |            |
|                                                         | 1                                                                                                                                                                                                                                                                                                                                                                                                                   | Ciała skończone, rozszerzenie ciała                                                                                                                                                                          | 2       |           |             |                                                 |               |            |
|                                                         | 2                                                                                                                                                                                                                                                                                                                                                                                                                   | Elementy algebraiczne, wielomian minimalny                                                                                                                                                                   | 2       | 1         |             |                                                 |               |            |
|                                                         | 3                                                                                                                                                                                                                                                                                                                                                                                                                   | Rozszerzenia algebraiczne                                                                                                                                                                                    | 2       | 1         |             |                                                 |               |            |
|                                                         | 4                                                                                                                                                                                                                                                                                                                                                                                                                   | Istnienie i izomorfizm ciał skończonych, ciało rozkładu wielomianu                                                                                                                                           | 2       | 2         |             |                                                 |               |            |
|                                                         | 5                                                                                                                                                                                                                                                                                                                                                                                                                   | Pierwiastki z jedynki                                                                                                                                                                                        | 2       |           |             |                                                 |               |            |
|                                                         | 6                                                                                                                                                                                                                                                                                                                                                                                                                   | wielomiany cyklotomiczne                                                                                                                                                                                     | 4       | 2         |             |                                                 |               |            |
|                                                         | 7                                                                                                                                                                                                                                                                                                                                                                                                                   | Konstrukcja ciał Galois                                                                                                                                                                                      | 2       | 2         |             |                                                 |               |            |
|                                                         | 8                                                                                                                                                                                                                                                                                                                                                                                                                   | Bazy normalne                                                                                                                                                                                                | 2       |           |             |                                                 |               |            |
|                                                         | 9                                                                                                                                                                                                                                                                                                                                                                                                                   | konstrukcja baz normalnych                                                                                                                                                                                   | 2       |           |             |                                                 |               |            |
|                                                         | 10                                                                                                                                                                                                                                                                                                                                                                                                                  | Praca kontrolna                                                                                                                                                                                              |         | 2         |             |                                                 |               |            |
|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                     | Razem                                                                                                                                                                                                        | 20      | 10        |             |                                                 |               |            |
| Literatura                                              | podstawowa:<br>● A. Białynicki-Birula, Algebra, PWN, 1976.<br>● J. Browkin, Teoria ciał, PWN, 1977.<br>● J. Gawinecki, J. Szmidt, Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii, WAT, 2002 uzupełniająca:<br>● R Lidl, H. Niederreiter, Finite Fields, PWN, 1984.                                                                                                                            |                                                                                                                                                                                                              |         |           |             |                                                 |               |            |
| Efekty uczenia się                                      | Symbol                                                                                                                                                                                                                                                                                                                                                                                                              | Efekty kształcenia                                                                                                                                                                                           |         |           |             | odniesienie do efektów kształcenia dla kierunku |               |            |
|                                                         | W01                                                                                                                                                                                                                                                                                                                                                                                                                 | Posiada podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania przedmiotów specjalistycznych, które wykorzystują pojęcia związane z teorią ciał skończonych, teorią Galois oraz bazami normalnymi. |         |           |             | K_W02                                           |               |            |
|                                                         | W02                                                                                                                                                                                                                                                                                                                                                                                                                 | Zna pojęcie ciała skończonego oraz liczbowego, charakterystyki ciała oraz ideału maksymalnego, który służy do konstrukcji rozszerzenia ciała. Zna pojęcie bazy normalnej w ciele skończonym.                 |         |           |             | K_W02                                           |               |            |
|                                                         | W03                                                                                                                                                                                                                                                                                                                                                                                                                 | Zna pojęcie elementu algebraicznego i elementu przestępnego oraz pierwiastka pierwotnego z jedynki. Zna podstawowe fakty związane z pojęciem wielomianu cyklotomicznego nad ciałem skończonym.               |         |           |             | K_W02                                           |               |            |
|                                                         | U01                                                                                                                                                                                                                                                                                                                                                                                                                 | Umie wyznaczyć wielomian minimalny elementu algebraicznego. Potrafi wyznaczyć ciało rozkładu wielomianu nad ciałem                                                                                           |         |           |             | K_U03                                           |               |            |

|                                                                                                                | Symbol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Efekty kształcenia                                                                                                                                                                                                                                                                          | odniesienie do efektów kształcenia dla kierunku |  |
|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|--|
|                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | skończonym i ciałem liczb wymiernych.                                                                                                                                                                                                                                                       |                                                 |  |
|                                                                                                                | U02                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Umie konstruować rozszerzenia ciał skończonych za pomocą wielomianów cyklotomicznych.                                                                                                                                                                                                       | K_U03                                           |  |
|                                                                                                                | U03                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Umie pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie. | K_U03                                           |  |
|                                                                                                                | K01                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze złożoną strukturą matematyki.                                                                                                                                                                | K_U03                                           |  |
| Metody i kryteria oceniania<br>(sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się) | <ul style="list-style-type: none"><li>• Przedmiot zaliczany jest na podstawie zaliczenia sprawdzającego wiedzę (W01, W02 i W03) i umiejętności (U01 i U02). Zaliczenie przeprowadzane jest w formie pisemnej lub pisemnej i ustnej. Warunkiem dopuszczenia do zaliczenia jest zaliczenie ćwiczeń rachunkowych.</li><li>• Ćwiczenia rachunkowe zaliczane są na podstawie wyników prac kontrolnych przeprowadzanych pod bezpośrednią kontrolą podczas zajęć (U01, U02, W01, W02, W03) lub w formie zadań do samodzielnego rozwiązania (U01, U02, U03).</li><li>• Dodatkowo studenci otrzymują wskazówki do samodzielnego studiowania z zachętą do korzystania z różnorodnych źródeł wiedzy (U03 i K01).</li><li>• Skala ocen: dostatecznie (3) - student zna i rozumie większość wyłożonych zagadnień, umie rozwiązywać najprostsze zadania rachunkowe, rozumie treść najważniejszych twierdzeń; dobrze (4) - student zna i rozumie znaczną większość wyłożonych zagadnień, umie formułować i rozwiązywać najprostsze zadania rachunkowe oraz interpretować ich wyniki za pomocą twierdzeń; bardzo dobrze (5) - student zna i rozumie wszystkie wyłożone zagadnienia, umie formułować i rozwiązywać zadania rachunkowe oraz interpretować ich wyniki za pomocą twierdzeń; dość dobrze (3,5) i ponad dobrze (4,5) - pośrednio między dostatecznie i dobrze oraz między dobrze i bardzo dobrze.</li></ul> |                                                                                                                                                                                                                                                                                             |                                                 |  |
| Bilans ECTS<br>(nakład pracy studenta)                                                                         | SEMESTR 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                             |                                                 |  |
|                                                                                                                | Aktywność                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Obciążenie studenta                                                                                                                                                                                                                                                                         |                                                 |  |
|                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Liczba godzin                                                                                                                                                                                                                                                                               | Liczba ECTS                                     |  |
|                                                                                                                | Udział w wykładach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 20                                                                                                                                                                                                                                                                                          | 1                                               |  |
|                                                                                                                | Udział w laboratoriach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0                                                                                                                                                                                                                                                                                           | 0                                               |  |
|                                                                                                                | Udział w ćwiczeniach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 10                                                                                                                                                                                                                                                                                          | 1                                               |  |
|                                                                                                                | Udział w projektach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0                                                                                                                                                                                                                                                                                           | 0                                               |  |
|                                                                                                                | Udział w seminariach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 0                                                                                                                                                                                                                                                                                           | 0                                               |  |
|                                                                                                                | Samodzielne studiowanie tematyki wykładów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 30                                                                                                                                                                                                                                                                                          | 0.5                                             |  |
|                                                                                                                | Samodzielne przygotowanie do laboratoriów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 30                                                                                                                                                                                                                                                                                          | 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 90                                                                                                                                                                                                                                                                                          | 3                                               |  |
|                                                                                                                | Zajęcia z udziałem nauczycieli                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 30                                                                                                                                                                                                                                                                                          | 2                                               |  |
|                                                                                                                | Zajęcia powiązane z działalnością naukową                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 90                                                                                                                                                                                                                                                                                          | 3                                               |  |
|                                                                                                                | Zajęcia o charakterze praktycznym                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 40                                                                                                                                                                                                                                                                                          | 1.5                                             |  |

autor

kierownik jednostki organizacyjnej  
odpowiedzialnej za przedmiot

dr Piotr Kacprzyk

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Koidecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis