

1.	Nazwa kierunku	informatyka stosowana
2.	Wydział	Wydział Nauk Ścisłych i Technicznych
3.	Cykl rozpoczęcia	2023/2024 (semestr zimowy), 2024/2025 (semestr zimowy)
4.	Poziom kształcenia	studia pierwszego stopnia (inżynierskie)
5.	Profil kształcenia	ogólnoakademicki
6.	Forma prowadzenia studiów	stacjonarna

7.	Informacje podstawowe o module	
Nazwa modułu		Matematyka dyskretna z elementami kryptografii
Kod modułu		W4-IS-S1-MDEK
Liczba punktów ECTS		5
Język wykładowy		polski
Cel i opis treści kształcenia		Celem przedmiotu jest zaznajomienie z zagadnieniami związanymi z matematyką dyskretną oraz przedstawienie podstaw teoretycznych współczesnej kryptografii a także przedstawienie głównych problemów dotyczących kryptografii wraz z odpowiednimi algorytmami stosowanymi w rozwiązaniach. Realizowane treści: 1. Elementy teorii liczb: liczby pierwsze, jednoznaczność rozkładu, NWD, algorytm Euklidesa, równania diofantyczne; kongruencje, arytmetyka modularna, ciała skończone, logarytm dyskretny, małe twierdzenie Fermata i twierdzenie Eulera; sito Eratostenesa, testy pierwszości, algorytm Rabina, rozkład liczby na czynniki, algorytm Fermata. 2. Elementy kryptografii: problem logarytmu dyskretnego, szyfr Cezara, algorytm szyfrujący RSA, algorytm ElGamala i warunki ich bezpieczeństwa, protokół Diffiego - Hellmana. Funkcja skrótu, podpis cyfrowy i uwierzytelnianie. 2. Kombinatoryka: wariacje, permutacje, kombinacje; symbole dwumianowe Newtona i ich własności. Algorytmy generujące proste obiekty kombinatoryczne: permutacje, wariacje, podzbiory zbioru; generowanie losowych obiektów kombinatorycznych; złożoność obliczeniowa i przykłady zastosowań takich algorytmów. 3. Metody zliczania obiektów: metoda bijektywna; reguła włączania i wyłączania; rekurencja i funkcje tworzące, liczby Fibonacciego. 4. Elementy teorii grafów: podstawowe pojęcia; minimalne drzewo rozpinające; problem minimalnych odległości; grafy Eulera i Hamiltona, problem komiwojażera.
Lista modułów koniecznych do zaliczenia przed przystąpieniem do tego modułu (o ile to konieczne)		nie dotyczy

8.	Zakładane efekty uczenia się modułu			
Kod	Opis	Efekty uczenia się kierunku	Stopień realizacji (skala 1-5)	
W4-IS-S1-MDEK_01	zna i rozumie znaczenie zastosowań matematyki dyskretniej w informatyce	IS1_W01	4	
		IS1_W02	3	
W4-IS-S1-MDEK_02	zna podstawowe pojęcia i metody obliczeniowe elementarnej teorii liczb	IS1_W01	4	
		IS1_W02	4	

W4-IS-S1-MDEK_03	zna i opisuje szyfry klasyczne oraz podstawowe kryptosystemy z kluczem publicznym i wyjaśnia matematyczne podstawy ataku na nie	IS1_W01 IS1_W03	3 3
W4-IS-S1-MDEK_04	zna pojęcia kombinatoryki i algorytmy kombinatoryczne	IS1_W02	4
W4-IS-S1-MDEK_05	zna pojęcia związane z teorią grafów	IS1_W01	3
W4-IS-S1-MDEK_06	potrafi zastosować algorytm Euklidesa do rozwiązywania równań diofantycznych liniowych i układów równań kongruencyjnych, potrafi zastosować poznane metody testowania liczb pierwszych i rozkładu liczb na czynniki pierwsze	IS1_U01 IS1_U05	3 4
W4-IS-S1-MDEK_07	potrafi analizować ataki na RSA i wyjaśnić podstawy matematyczne ataków na szyfry klasyczne i szyfry asymetryczne	IS1_U01 IS1_U08	3 4
W4-IS-S1-MDEK_08	potrafi zastosować właściwe schematy kombinatoryczne do rozwiązywania problemów informatycznych i przeprowadzić konieczne obliczenia przy pomocy poznanych metod i algorytmów	IS1_U01 IS1_U05	3 3
W4-IS-S1-MDEK_09	potrafi zastosować terminologię i algorytmy teorii grafów do rozwiązywania problemów informatycznych	IS1_U01 IS1_U05	3 3
W4-IS-S1-MDEK_10	jest świadom istniejących zagrożeń dla bezpieczeństwa informacji	IS1_K01 IS1_U08	3 3

9. Metody prowadzenia zajęć		
Kod	Kategoria	Nazwa (opis)
a01	Zbiór metod asymilacji wiedzy / podających	Wykład informacyjny/kursowy systematyczny kurs z określonej dyscypliny naukowej w ujęciu syntetycznym; realizacja zakłada bierny odbiór przekazanych informacji
b08	Zbiór metod problemowych	Metody aktywizujące: peer learning nauka poprzez wymianę wiedzy w grupie/zespole/parze czyli tzw. komórce nauczania (ang. learning cells); rodzaj uczenia się wzajemnie od siebie; podejście skoncentrowane na aktywności studentów z towarzyszeniem NA prowadzącego zajęcia; nauczanie, w ramach którego studenci o podobnym poziomie doświadczenia uczą się od siebie nawzajem
c07	Zbiór metod eksponujących	Prezentacja mechaniczne przedstawienie syntetycznego obrazu treści w formie grafiki prezentacyjnej, np. szeregu slajdów lub innych form multimedialnych zwykle z omówieniem/innym komentarzem; typowe składniki prezentacji - tekst ujęty w punkty, wykresy, grafika (obrazy) i animacje; ew. efekty dźwiękowe lub muzyka; ilustracja multimedialna treści zajęć prezentowana w formie rzutowanego obrazu
e01	Zbiór metod praktycznych	Ćwiczenie laboratoryjne/doświadczenie [w tym, w terenie] metoda praktycznego stosowania wiedzy; realizowana w trzech fazach: dostrzeżenie problemu wywołanego treścią zadania, sformułowanie problemu i próba samodzielnego rozwiązania z oceną skutków; celem jest zdobycie umiejętności, sprawności i nawyków oraz utrwalenie posiadanych wiadomości, tak aby wiedza stała się wiedzą operatywną; metoda laboratoryjna zakłada większą niż przeprowadzenie doświadczenia samodzielność uczących się

10. Formy prowadzonych zajęć					
Kod	Nazwa	Liczba godzin	Sposób weryfikacji efektów uczenia się	Efekty uczenia się modułu	Metody prowadzenia zajęć
IS-S1-MDEK_fs_1	wykład	15	egzamin	W4-IS-S1-MDEK_01, W4-IS-S1-MDEK_02, W4-IS-S1-MDEK_03, W4-IS-S1-MDEK_04, W4-IS-S1-MDEK_05	a01, c07
IS-S1-MDEK_fs_2	konwersatorium	45	zaliczenie	W4-IS-S1-MDEK_06, W4-IS-S1-MDEK_07, W4-IS-S1-MDEK_08, W4-IS-S1-MDEK_09, W4-IS-S1-MDEK_10	b08, e01

11. Praca studenta poza udziałem w zajęciach obejmuje w szczególności:			
Kod	Kategoria	Nazwa (opis)	Czy częściowo zalicza się do BUNA-y?
a02	Przygotowanie do zajęć	Czytanie literatury / analiza materiałów źródłowych <i>czytanie literatury wskazanej w sylabusie; przegląd, porządkowanie, analiza i wybór materiałów źródłowych do wykorzystania w ramach zajęć</i>	Nie
a03	Przygotowanie do zajęć	Ćwiczenie praktycznych umiejętności <i>czynności polegające na powtarzaniu, doskonaleniu i utrwalaniu praktycznych umiejętności, w tym ćwiczonych podczas odbytych wcześniej zajęć lub nowych, niezbędnych z punktu widzenia realizacji kolejnych elementów programu (jako przygotowanie się uczestnictwa w zajęciach)</i>	Nie
a04	Przygotowanie do zajęć	Konsultowanie materiałów uzupełniających [względem wskazanych w sylabusie] <i>uzgadnianie dodatkowych do wskazanych w sylabusie materiałów, służących realizacji zadań wynikających z uczestnictwa w zajęciach lub na potrzeby przygotowania się do nich</i>	Tak
c01	Przygotowanie do weryfikacji efektów uczenia się	Ustalanie etapów realizacji zadań przyczyniających się do weryfikacji efektów uczenia się <i>przygotowanie strategii realizacji zadania uwzględniającej podział treści, czynności i ich zakres, czas realizacji oraz/lub sposób pozyskania niezbędnych do jego wykonania materiałów i narzędzi, itp.</i>	Tak
c02	Przygotowanie do weryfikacji efektów uczenia się	Studiowanie wykorzystanej literatury oraz wytworzonych w ramach zajęć materiałów <i>wglębianie się, dociekanie, rozważanie, przyswajanie, interpretacja lub porządkowanie wiedzy pochodzącej z literatury, dokumentacji, instrukcji, scenariuszy, itd., wykorzystanych na zajęciach oraz z notatek lub innych materiałów/wytworów sporządzonych w ich trakcie</i>	Nie
d01	Konsultowanie wyników weryfikacji efektów uczenia się	Analiza korekt/informacji zwrotnej ze strony NA dotyczących wyników wer. ef. ucz. <i>przegląd uwag, ocen i opinii sporządzonych przez NA odnoszących się do realizacji zadania sprawdzającego poziom osiągniętych efektów uczenia się</i>	Tak
d02	Konsultowanie wyników weryfikacji efektów uczenia się	Opracowanie planu korekty i zadań uzupełniających/korygujących <i>przegląd i wybór zadań oraz czynności pozwalających na eliminację wskazanych przez NA błędów, ich weryfikację lub poprawę oraz zaliczenie zadania na, co najmniej, najniższym dopuszczalnym poziomie</i>	Tak

Informacje dotyczące szczegółów realizacji modułu w danym roku akademickim znajdują się w sylabusie dostępnym w systemie USOS: <https://usosweb.us.edu.pl>.