

1.	Nazwa kierunku	matematyka
2.	Wydział	Wydział Nauk Ścisłych i Technicznych
3.	Cykl rozpoczęcia	2025/2026 (semestr zimowy)
4.	Poziom kształcenia	studia drugiego stopnia
5.	Profil kształcenia	ogólnoakademicki
6.	Forma prowadzenia studiów	stacjonarna

7.	Informacje podstawowe o module	
Nazwa modułu		Elementy kryptografii
Kod modułu		W4-MT-S2-23-WKry
Liczba punktów ECTS		3
Język wykładowy		polski
Cel i opis treści kształcenia		Celem przedmiotu jest przedstawienie głównych pojęć związanych z kryptografią oraz problemów dotyczących zagadnień kryptograficznych wraz z algorytmami stosowanymi w rozwiązaniach. W szczególności omówione zostaną: główne pojęcia kryptografii i kryptoanalizy (szyfrowanie, deszyfrowanie, klucz, bezpieczeństwo, itp.) kryptografia klasyczna (szyfr Cezara, szyfr Vigenere'a, szyfry mono- i polialfabetyczne, itp), szyfrowanie asymetryczne (RSA, ElGamal) podpisy cyfrowe, funkcje skrótu, zadania autoryzacji, weryfikacji, teoria informacji. Dodatkowo, na zajęciach rozwinięte zostaną umiejętności dydaktycznego przekazywania na poziomie szkoły ponadpodstawowej. Przyszli nauczyciele zostaną przygotowani do nauczania elementów bezpieczeństwa cyfrowego i kryptografii w kontekście szkolnym oraz realizacji podstawy programowej z informatyki.
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)
EKry_01	student zna pojęcia i metody kryptografii klasycznej i współczesnej,	KN_NI_W10 K_W05	5 2
EKry_02	student rozumie znaczenie funkcji skrótu, podpisów cyfrowych i certyfikatów,	KN_NI_W10 K_W05	5 2
EKry_03	student zna metodykę nauczania zagadnień związanych z kryptografią w szkole	KN.2023_W15 KN_NI_W10	3 2

EKry_04	student potrafi szyfrować i deszyfrować w określonym systemie kryptograficznym	K_U05	2
EKry_05	student potrafi wyjaśnić uczniom mechanizmy szyfrowania i bezpieczeństwa w przystępny sposób	KN.2023_U07	2
EKry_06	student jest gotów do stosowania zasad zabezpieczenia danych	K_K07	1
EKry_07	wykazuje świadomość odpowiedzialności nauczyciela w zakresie edukacji cyfrowej i ochrony danych	K_K03	1

9. Metody prowadzenia zajęć		
Kod	Kategoria	Nazwa (opis)
b02	Zbiór metod problemowych	Wykład konwersatoryjny <i>przekaz treści uwzględniający interakcję ze słuchaczami wykładu; dyskusja związana z wykładem stanowi jeden z jego elementów bądź jest jego kontynuacją</i>
b08	Zbiór metod problemowych	Metody aktywizujące: peer learning <i>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</i>
b09	Zbiór metod problemowych	Metody aktywizujące: flipped classroom <i>nauczanie wyprzedzające; praca na zajęciach opiera się na uprzednio samodzielnie przestudiowanym materiale wskazanym przez prowadzącego zajęcia; przygotowanie poza zajęciami służy poznaniu zagadnień stanowiących warunek uczestnictwa w dyskusji oraz ćwiczenia powiązanych z nimi umiejętności praktycznych; ciężar aktywności opiera się na pracy studentów z towarzyszeniem prowadzącego zajęcia</i>
c07	Zbiór metod eksponujących	Prezentacja <i>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</i>
d03	Zbiór metod programowanych	Praca z innym narzędziem dydaktycznym <i>np. z wykorzystaniem stron internetowych w dowolny sposób lub wg reguł ustalonych przez prowadzącego zajęcia; lub inne, specyficzne dla przedmiotu studiów</i>

10. Formy prowadzonych zajęć					
Kod	Nazwa	Liczba godzin	Sposób weryfikacji efektów uczenia się	Efekty uczenia się modułu	Metody prowadzenia zajęć
EKry_fs_01	wykład	15	zaliczenie	EKry_01, EKry_02, EKry_03, EKry_04, EKry_06, EKry_07	b02, c07
EKry_fs_02	konwersatorium	30	zaliczenie	EKry_01, EKry_04, EKry_05, EKry_06, EKry_07	b08, b09, d03

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
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>wgłębianie 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

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