

KARTA KURSU

Nazwa	Kryptografia
Nazwa w j. ang.	Kryptography

Koordynator	dr hab. prof. Oleksandr Korchenko	Zespół dydaktyczny
		dr hab. prof. Oleksandr Korchenko
Punktacja ECTS*	4	

Opis kursu (cele kształcenia)

Celem tego kursu jest zapoznanie studentów z historią, podstawowymi zasadami, metodami i zaawansowanymi technikami kryptografii i kryptoanalizy oraz umożliwienie im zdobycia głębokiego zrozumienia zasad szyfrowania, bezpieczeństwa danych i protokołów kryptograficznych, aby wyposażyć ich w niezbędną wiedzę i umiejętności do projektowania, implementacji i analizy systemów zabezpieczeń informatycznych. Kurs jest realizowany w języku polskim.

Warunki wstępne

Wiedza	Znajomość analizy matematycznej i algebry. Podstawowe metodologie tworzenia oprogramowania.
Umiejętności	Umiejętność programowania i samodzielnego korzystania z literatury przedmiotu.
Kursy	Wybrane zagadnienia matematyki wyższej.

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student:	
	W01: Zna historię, podstawowe pojęcia i definicje kryptologii.	K_W01, K_W02
	W02: Zna podstawowe elementy kryptografii.	K_W01 K_W03
	W03: Zna kryptograficzne algorytmy symetryczne i tryby działań.	K_W03, K_W05,
	W04: Zna kryptograficzne protokoły i algorytmy asymetryczne.	K_W05, K_W06
	W05: Zna funkcje skrótu i podpis cyfrowy.	K_W05, K_W06
	W06: Zna techniki i metody kryptoanalizy.	K_W01, K_W07
	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student:	
	U01: Potrafi projektować i implementować podstawowe kryptosystemy symetryczne i asymetryczne.	K_U03, K_U04, K_U06, K_U07
	U02: Umie korzystać się protokołów kryptograficznych.	K_U07, K_U08
	U03: Potrafi korzystać się literaturą z zakresu teorii kryptografii i kryptoanalizy.	K_U12, K_U13

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student: K01: potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania. K02: rozumie potrzebę kształcenia ustawicznego i śledzenia na bieżąco zmian w zakresie standardów odnoszących się do nowoczesnych algorytmów kryptograficznych.	K_K01, K_K02 K_K01, K_K02

Studia stacjonarne

Organizacja							
Forma zajęć	Wykład (W)	Ćwiczenia w grupach					
		A	K	L	S	P	E
Liczba godzin	20			20			

Studia niestacjonarne

Organizacja							
Forma zajęć	Wykład (W)	Ćwiczenia w grupach					
		A	K	L	S	P	E
Liczba godzin	15			15			

Opis metod prowadzenia zajęć

1. Wykłady: Podczas wykładów prowadzący przedstawiają materiał teoretyczny, wyjaśniają kluczowe koncepcje i metody oraz prezentują przykłady, ilustracje, slajdy i filmy. Wykłady mogą być prowadzone w auli lub online, a nagrania z nich mogą być udostępniane do późniejszego obejrzenia.
2. Ćwiczenia laboratoryjne: Ćwiczenia laboratoryjne pozwalają studentom przeprowadzać praktyczne eksperymenty z rzeczywistymi danymi, które pomagają studentom utrwalić wiedzę teoretyczną.
3. Dyskusje i zadania grupowe: Dyskusje i zadania grupowe promują wymianę wiedzy między studentami i zachęcają do wspólnego uczenia się. Metody te mogą obejmować forum dyskusyjne, grupowe projekty oraz wspólne rozwiązywanie zadań.
4. Samodzielne uczenie się: Dodatkowo, studentom mogą być udostępniane materiały do samodzielnego uczenia się, takie jak podręczniki, artykuły i kursy online. To pozwala studentom na pogłębienie swojej wiedzy i badanie tematów, które ich szczególnie interesują.
5. Testy i ocena: W trakcie kursu studenci mogą przechodzić testy i prace kontrolne w celu oceny swojego poziomu wiedzy i osiągnięć. Oceny te mogą obejmować zarówno egzaminy pisemne, jak i ocenę wyników ćwiczeń laboratoryjnych.

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01					X								
W02					X								
W03					X								
W04					X								
W05					X								
W06					X								
U01					X			X					
U02					X			X					
U03					X			X					
K01					X			X					
K02					X			X					

Kryteria oceny	<p>Zaliczenie na ocenę dostateczną otrzymuje student, który potrafi: samodzielnie wykonać minimalną liczbę zadań (samodzielnie tworzy oprogramowanie oraz analizuje warunki i obszary zastosowania testowanych algorytmów) oraz udzielić poprawnej odpowiedzi na minimalną liczbę pytań testowych.</p> <p>Zaliczenie na ocenę dobrą lub bardzo dobrą otrzymuje student, który spełnia warunki oceny dostatecznej, a oprócz tego także: samodzielnie wykona większą liczbę zadań oraz udzieli poprawnej odpowiedzi na większą liczbę pytań testowych.</p> <p>Ocena końcowa zależy od ocen częściowych i regularności wykonywania zadań.</p>
----------------	--

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

<ol style="list-style-type: none"> Historia kryptografii: <ul style="list-style-type: none"> - Steganografia; - Kryptografia; - Rozwój kryptografii i kryptoanalizy; - Kryptografia II wojny światowej; - Era komputerów. Podstawowe elementy kryptografii: <ul style="list-style-type: none"> - Podstawowe pojęcia; - Proste szyfry; - Szyfrowanie z kluczem; - Szyfrowanie symetryczne; - Szyfrowanie asymetryczne. Kryptograficzne algorytmy symetryczne: <ul style="list-style-type: none"> - Data Encryption Standard; - Triple DES; - Algorytm Blowfish; - Algorytmy z rodziny CAST; - International Data Encryption Algorithm; - Algorytmy RC2, RC4, RC5, RC6; - Algorytm Rijndael; - Advanced Encryption Standard. Tryby działań algorytmów symetrycznych: <ul style="list-style-type: none"> - Uwagi ogólne; - Tryb elektronicznej książki kodowej (ECB); - Tryb wiązania bloków zaszyfrowanych (CBC); - Szyfry strumieniowe;
--

- Tryb sprzężenia zwrotnego szyfrogramu (CFB);
- Tryb sprzężenia zwrotnego wyjściowego (OFB);
- Tryb licznikowy
- Inne tryby działań symetrycznych szyfrów blokowych;
- Zastosowania trybów pracy symetrycznych algorytmów kryptograficznych.
5. Algorytm kryptograficzny RSA:
- Schemat i opis algorytmu;
- Procedura szyfrowania i odszyfrowania;
- Stosowanie.
6. Funkcja skrótu:
- Funkcje jednokierunkowe;
- MD4 i MD5;
- SHA-1, SHA-2 i SHA-3.
7. Podpis cyfrowy:
- Uogólniony schemat;
- ElGamala;
- DSA;
- Ślepe podpisy cyfrowe;
- Niezaprzeczalne podpisy cyfrowe.
8. Techniki i metody kryptoanalityczne:
- Kryptoanaliza;
- Techniki łamania szyfrów;
- Łamanie szyfru.

Wykaz literatury podstawowej

1. M. Karbowski, Podstawy kryptografii, Wydanie III. Helion 2021, Gliwice, 2021, str 328.
2. Douglas R. Stinson, Maura B. Paterson, Kryptografia w teorii i praktyce, Wydanie IV. Wydawnictwo Naukowe PWN SA, Warszawa, 2021, 555 str.
3. Jean-Philippe Aumasson, Nowoczesna kryptografia, Praktyczne wprowadzenie do szyfrowania. Wydawnictwo Naukowe PWN SA, Warszawa, 2018, 320 str.
4. Internet-strony www wskazane na wykładzie.

Wykaz literatury uzupełniającej

1. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii, Gliwice, Helion, 2012.
2. N.Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa, 2006.
3. R.A.Mollin, RSA and Public-Key Cryptography, Chapman Hall CRC, 2003.
4. W. Trappe, L.C. Washington, Introduction to cryptography with Coding Theory, Prentice Hall, 2002

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia stacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	20
	Konwersatorium (ćwiczenia, laboratorium itd.)	20
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	35
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		100
Liczba punktów ECTS w zależności od przyjętego przelicznika		4

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia niestacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	45
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		100
Liczba punktów ECTS w zależności od przyjętego przelicznika		4