

KARTA KURSU

Nazwa	Podstawy Kryptografii
Nazwa w j. ang.	Kryptography fundamentals

Koordynator	dr hab. prof. uken Oleksandr Korchenko	Zespół dydaktyczny
		dr hab. prof. Oleksandr Korchenko
Punktacja ECTS*	5	

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 wyposażać 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.	SC_W01
	W02: Zna podstawowe elementy kryptografii.	SC_W01
	W03: Zna kryptograficzne algorytmy symetryczne i tryby działań.	SC_W01, SC_W02
	W04: Zna kryptograficzne protokoły i algorytmy asymetryczne.	SC_W01, SC_W02
	W05: Zna funkcje skrótu i podpis cyfrowy. W06: Zna techniki i metody kryptoanalizy.	SC_W01, SC_W02 SC_W01

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	<p>Po zakończeniu kursu student:</p> <p>U01: Potrafi projektować i implementować podstawowe kryptosystemy symetryczne i asymetryczne.</p> <p>U02: Umie korzystać się protokołów kryptograficznych.</p> <p>U03: Potrafi korzystać się literaturą z zakresu teorii kryptografii i kryptoanalizy.</p>	<p>SC_U01, SC_U02, SC_U04</p> <p>SC_U01, SC_U04, SC_U05</p> <p>SC_U01, SC_U02, SC_U04, SC_U05</p>

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	<p>Po zakończeniu kursu student:</p> <p>K01: potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania.</p> <p>K02: rozumie potrzebę kształcenia ustawicznego i śledzenia na bieżąco zmian w zakresie standardów odnoszących się do nowoczesnych algorytmów kryptograficznych.</p>	<p>SC_K01</p> <p>SC_K02</p>

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	30	30									

Studia niestacjonarne

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

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	Ocena końcowa jest zależna od ocen cząstkowych, systematyczności realizowanych zadań oraz oceny uzyskanej za realizację projektu zespołowego (indywidualnego). W szczególności ocenę dobrą i bardzo dobrą z ćwiczeń może uzyskać student, który: samodzielnie tworzy oprogramowanie wykorzystujące omawiane techniki przetwarzania sygnałów, potrafi zanalizować warunki i obszary stosowalności testowanych algorytmów.
----------------	--

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

<p>1. Historia kryptografii:</p> <ul style="list-style-type: none"> - Steganografia; - Kryptografia; - Rozwój kryptografii i kryptoanalizy; - Kryptografia II wojny światowej; - Era komputerów. <p>2. Podstawowe elementy kryptografii:</p> <ul style="list-style-type: none"> - Podstawowe pojęcia; - Proste szyfry; - Szyfrowanie z kluczem; - Szyfrowanie symetryczne; - Szyfrowanie asymetryczne.
--

3. Kryptograficzne algorytmy symetryczne:
 - 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.
4. Tryby działań algorytmów symetrycznych:
 - 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. Krzywe eliptyczne:
 - Podstawowe pojęcia;
 - Kryptografia na krzywych eliptycznych.
9. Techniki i metody kryptoanalityczne:
 - Kryptoanaliza;
 - Techniki łamania szyfrów;
 - Łamanie szyfru.

Wykaz literatury podstawowej

1. M. Karbowski, Podstawy kryptografii. Wydanie III, Helion 2014.
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. L.C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition, Chapman Hall CRC, 2008.
5. 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. 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	30
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	40
	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		125
Liczba punktów ECTS w zależności od przyjętego przelicznika		5

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

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	60
	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		125
Liczba punktów ECTS w zależności od przyjętego przelicznika		5