

KARTA KURSU (realizowanego w module specjalności)
Cyberbezpieczeństwo

Nazwa	Zaawansowane metody kryptografii
Nazwa w j. ang.	Advanced cryptography methods

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

Opis kursu (cele kształcenia)

Celem tego kursu jest zapoznanie studentów z 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 podstawowe pojęcia i definicje kryptologii. W02: Zna matematyczne podstawy kryptografii. W03: Zna zaawansowane kryptograficzne algorytmy. W04: Zna kryptograficzne protokoły. W05: Zna funkcje skrótu i podpis cyfrowy. W06: Zna techniki i metody kryptoanalityczne.	SC_W01 SC_W01, SC_W04 SC_W01 SC_W01, SC_W04 SC_W01 SC_W01, SC_W04
Umiejętności	Po zakończeniu kursu student: U01: Potrafi projektować i implementować podstawowe kryptosystemy symetryczne i asymetryczne. U02: Umie korzystać się protokołów kryptograficznych. U03: Potrafi korzystać się literaturą z zakresu teorii kryptografii i kryptoanalizy.	SC_U01, SC_U02 SC_U01, SC_U03 SC_U01, SC_U07

Kompetencje społeczne	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	<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. Kryptografia Matematyczna:</p> <ul style="list-style-type: none"> - Słownik tekstu jawnego; - Przestrzeń tekstu; - Iloczyn kartezjański; - System kryptograficzny; - Szyfrowanie monoalfabetyczne i polialfabetyczne; - Funkcje jednokierunkowe; - Arytmetyka modulo; - Liczby pierwsze (Sito Eratostenesa, Sundarama i Atkina, Liczby Mersenne’a, Małe twierdzenie Fermata, NWD i NWW); - Grupy, pierścienie i ciała (Grupa, Pierścień, Ciało); - Izomorfizmy (Funkcja różnowartościowa, Surjekcja, Przekształcenie izomorficzne). <p>2. Matematyczne aspekty rozwiązań kryptograficznych:</p> <ul style="list-style-type: none"> - Kryptosystem RSA; - Problem faktoryzacji dużych liczb; - Mocne liczby pierwsze; - Generowanie liczb pierwszych (Test Lehmana, Rabina-Millera, Solovaya-Strassena i Fermata); - Chińskie twierdzenie o resztach; - Logarytm dyskretny; - Złożoność algorytmów; - Pojęcia i wzory Shannona (Entropia, Nadmiarowość i zawartość informacyjna języka, Odległość jednostkowa, Mieszanie i rozpraszanie). <p>3. Ataki kryptoanalityczne:</p> <ul style="list-style-type: none"> - Metody kryptoanalityczne; - Kryptoanaliza liniowa i różnicowa; - Inne rodzaje ataków. <p>4. Rodzaje i tryby szyfrowania:</p> <ul style="list-style-type: none"> - Szyfry blokowe;
--

- Tryby szyfrów blokowych;
 - Szyfry strumieniowe;
 - Generowanie ciągów pseudolosowych (Generatory kongruencyjne, Generatory oparte na rejestrze przesuwającym ze sprzężeniem zwrotnym, Generatory oparte na teorii złożoności, Generatory ciągów rzeczywiście losowych, Najpopularniejsze algorytmy strumieniowe).
5. Algorytmy szyfrujące:
- IDEA (Przekształcenia początkowe, Operacje pojedynczego cyklu IDEA, Generowanie podkluczy, Przekształcenia MA, Deszyfrowanie IDEA);
 - AES (Opis algorytmu, Generowanie kluczy, Rozszerzanie klucza, Selekcja podkluczy, Pojedyncza runda algorytmu (ByteSub, ShiftRow, MixColumn, AddRoundKey), Podsumowanie;
 - Twofish (Opis algorytmu, Pojedyncza runda algorytmu (Funkcja g, Przekształcenie PHT, Dodanie kluczy szyfrowania), Podsumowanie;
 - CAST5 (Opis algorytmu, Rundy CAST5);
 - Blowfish (Opis algorytmu, Funkcja algorytmu Blowfish);
 - DSA (Podpisywanie wiadomości, Weryfikacja podpisu, Wariant pierwszy DSA Wariant drugi DSA);
 - Inne algorytmy szyfrujące (RC2, RC5, RC6, GOST, BLOWFISH, REDOC, LOKI, SAFER, FEAL, CAST, Skipjack, MMB, 3-Way, CRAB, CA-1.1, Khufu i Khafre, algorytm Madrygi, NewDES, a także z kluczem publicznym plecakowe, ElGamala, Rabina, Pohliga-Hellmana, LUC i McEliece'a).
6. Krzywe eliptyczne:
- Podstawowe pojęcia;
 - Krzywe eliptyczne na liczbach całkowitych Dodawanie i mnożenie punktów;
 - Grupy punktów na krzywej eliptycznej;
 - Problem ECDLP;
 - Uzgadnianie klucza Diffiego-Hellmana na krzywych eliptycznych;
 - Podpisywanie z wykorzystaniem krzywych eliptycznych Generowanie podpisu ECDS;
 - Szyfrowanie z wykorzystaniem krzywych eliptycznych;
 - Wybór krzywej Krzywe NIST;
 - Curve25519;
 - Inne krzywe;
 - ECDSA z nieodpowiednią losowością;
 - Złamanie ECDSA za pomocą innej krzywej Inne źródła.
6. Protokoły kryptograficzne:
- Protokoły wymiany kluczy;
 - Protokół Diffiego-Hellmana;
 - KEA;
 - Wide-mouth frog;
 - Dzielenie sekretów (Sekret splitting i sharing);
 - Inne protokoły (Znakowanie czasowe, Dowody z wiedzą zerową, Kanały podprogowe, Protokoły uwierzytelniające).
7. Infrastruktura klucza publicznego:
- PKI w teorii i w praktyce;
 - Złożoność;
 - Zaufanie;
 - Cykl życia klucza.
8. Kryptografia alternatywna:
- Kryptografia DNA (Struktura DNA, Informatyka molekularna, Informacja ukryta w DNA, Szyfrowanie i deszyfrowanie z wykorzystaniem nukleotydów);
 - Kryptografia wizualna (Udziały, Schemat progowy).

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. 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. 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	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