Sylabus przedmiotu / modułu kształcenia – studia podyplomowe	
Nazwa przedmiotu/modułu kształcenia:	**Kryptografia i steganografia w praktyce**
Nazwa w języku angielskim:	**Cryptography and steganography in practice**
Język wykładowy:	Język polski
Studia podyplomowe dla których oferowany jest przedmiot/moduł kształcenia:	Studia Podyplomowe Cyberbezpieczeństwo
Dziedzina/dziedziny nauki, w ramach których prowadzone są studia podyplomowe:	Nauki Ścisłe i Przyrodnicze
Jednostka realizująca:	Wydział Nauk Ścisłych i Przyrodniczych
Rodzaj przedmiotu/modułu kształcenia (obowiązkowy/fakultatywny):	obowiązkowy
Rok studiów:	I
Semestr:	1
Liczba punktów ECTS:	3
Imię i nazwisko koordynatora przedmiotu:	dr Mirosław Szaban
Imię i nazwisko prowadzących zajęcia:	dr Mirosław Szaban
Założenia i cele przedmiotu:	Celem przedmiotu jest przedstawienie zagadnień realizowanych przez współczesną kryptografię i steganografię, podstawowych technik kryptograficznych, szyfrowania i deszyfrowania danych oraz przedstawienie standardowych algorytmów kryptograficznych praktyczne. Dla zrealizowania powyższego celu niezbędne jest również zapoznanie z podstawowymi działaniami matematycznymi z dziedziny teorii liczb.
Efekty uczenia się (wiedza, umiejętności, kompetencje społeczne):	WIEDZA: • Zna i rozumie w pogłębionym stopniu wiedzę z zakresu kryptografii i steganografii. • Zna i rozumie w pogłębionym stopniu najnowsze trendy rozwojowe z zakresu dziedzin nauki i dyscyplin naukowych związanych z kryptografią, kryptoanalizą, steganografią i zabezpieczaniem informacji.
	UMIEJĘTNOŚCI: • Potrafi właściwie dobrać źródła i pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać oceny, krytycznej analizy i syntezy tych informacji. • Potrafi dobrać oraz zastosować metody, algorytmy i narzędzia kryptograficzne oraz steganograficzne.

	KOMPETENCJE SPOŁECZNE: • Posiada umiejętność samodzielnego planowania i realizowania samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych. • Potrafi myśleć i działać w sposób przedsiębiorczy.
Forma i typy zajęć:	wykłady (10 godz.), ćwiczenia laboratoryjne (18 godz.)

Wymagania wstępne i dodatkowe:

Warunkiem uczestnictwa w zajęciach jest podstawowa znajomość obsługi komputera, oraz wiedza z zakresu logiki i teorii mnogości, algebry liniowej i matematyki dyskretnej.

Treści modułu kształcenia:

1. **Wprowadzenie do klasycznej kryptografii.** Pojęcia, definicje, podział technik kryptograficznych.
2. **Klasyczne szyfry.** Szyfr z przesunięciem. Szyfr podstawieniowy. Szyfr afiniczny. Szyfr Vigenère'a. Szyfr Hilla. Kryptoanaliza szyfru podsawieniowego. Kryptoanaliza szyfru afinicznego.Kryptoanaliza szyfru Vigenere'a. Ataki na szyfr Hilla.
3. **Teoria Shannona. Standard szyfrowania danych – algorytm DES. Kryptoanaliza różnicowa.** Tajność doskonała. Entropia. Własności entropii. Błędne klucze i długość krytyczna. Opis DES. Tryby działania DES. Wymagania czasowe a wymagania pamięciowe - próba kompromisu. Atak na 3-rundowy szyfr DES. Atak na 6-rundowy szyfr DES.
4. **Algorytm RSA. Ataki na RSA i system Rabina. Algorytmy faktoryzacji.** Wprowadzenie do kryptografii z kluczem publicznym. Elementy teorii liczb. System kryptograficzny RSA. Implementacje RSA. Wykładnik deszyfrowania. Częściowa informacja o bitach tekstu jawnego. System kryptograficzny Rabina. Metoda p – 1. Algorytm Dixona i sito kwadratowe. Algorytmy faktoryzacji w praktyce.
5. **Systemy kryptograficzne z kluczem publicznym. Schematy podpisów. Funkcje skrótu. Uzgadnianie i dystrybucja klucza.** System kryptograficzny ElGamala i logarytmy dyskretne. Systemy oparte na ciałach skończonych i krzywych eliptycznych. System plecakowy Merkle'a-Hellmana. System McEliece'a. Schemat podpisu ElGamala. Standard podpisu cyfrowego. Jednorazowe podpisy. Podpisy niezaprzeczalne. Bezkonfliktowe funkcje skrótu. Atak metodą dnia urodzin. Funkcja skrótu związana z logarytmem dyskretnym. Funkcje skrótu budowane na systemach kryptograficznych. Wstępna dystrybucja klucza. Kerberos. Protokół wymiany kluczy Diffiego Hellmana.
6. **Szyfrowanie obrazów.** Metody kryptograficzne stosowane do szyfrowania obrazów.Szyfrowanie obrazów w odcieniach szarości. Szyfrowanie obrazów z pełną gradacją kolorów.
7. **Steganografia.** Ukrywanie informacji. Steganografia a Kryptografia. Metoda najmniej istotnego bitu. Kompresja a steganografia. Steganografia z użyciem obrazów.
8. Metody i techniki współczesnej kryptografii i steganografii w zastosowaniach współczesnych.

Literatura podstawowa:

1. Stinson Douglas R., Kryptografia, W teorii i praktyce, WNT, 2004.
2. Andrzej Chrzęszczyk. Algorytmy teorii liczb i kryptografii w przykładach. BTC. 2010.
3. Rajesh Kumar, Steganografia obrazowa, Wydawnictwo Bezkresy Wiedzy, 2020

Literatura dodatkowa:

1. Neal Koblitz, Wykład z teorii liczb i kryptografii., WNT, 2015.

2. Marcin Karbowski, Podstawy kryptografii, Helion, 2014.

Planowane formy/działania/metody dydaktyczne:

Wykład tradycyjny wspomagany jest technikami multimedialnymi. Ćwiczenia laboratoryjne – zajęcia praktyczne z wykorzystaniem wybranych narzędzi programowych. Na stronie internetowej prowadzącego zamieszczane są materiały z problemami i zadaniami laboratoryjnymi.

Sposoby weryfikacji efektów uczenia się osiąganych przez studenta:

Efekty kształcenia z zakresu wiedzy weryfikowane będą poprzez egzamin pisemny, a także w toku przygotowania do kolejnych zajęć laboratoryjnych. Na egzaminie pytania będą dotyczyły poznanych algorytmów i technik kryptograficznych i steganograficznych, szyfrowania i deszyfrowania danych oraz poszukiwania ukrytych wiadomości. Przykładowe pytania egzaminacyjne:

- Przedstaw ideę systemu kryptograficznego symetrycznego.
- Przedstaw ideę systemu kryptograficznego z kluczem publicznym.
- Jakie są warunki osiągnięcia tajności doskonałej?
- Opisz system szyfrowania blokowego DES.

Przed egzaminem studenci będą mieli dostęp do przykładowych pytań na egzamin.
Efekty kształcenia z zakresu umiejętności i kompetencji społecznych będą sprawdzane systematycznie na zajęciach laboratoryjnych. Przykładowe zadania:

- Przedstaw działanie algorytmu RSA.
- Przedstaw szyfrowanie i deszyfrowane algorytmem IDEA.

Materiały na następne laboratorium będą dostępne na dwa dni przed zajęciami.

Forma i warunki zaliczenia (wraz z kryteriami oceniania):

Ocena z przedmiotu składa się z dwóch ocen cząstkowych:

- oceny z zajęć laboratoryjnych,
- oceny z egzaminu końcowego.

Na ocenę z zajęć laboratoryjnych składają się oceny cząstkowe uzyskane na regularnych zajęciach z nauczycielem akademickim, za które można uzyskać sumarycznie 40 pkt. Zaliczenie zajęć laboratoryjnych możliwe po uzyskaniu co najmniej 51% liczby punktów z tej formy zaliczenia

Egzamin jest egzaminem pisemnym. Do egzaminu mogą przystąpić osoby, które uzyskały zaliczenie laboratorium. Można na nim uzyskać maksymalnie 60 pkt. Egzamin będzie zaliczony w przypadku uzyskania co najmniej 51% liczby punktów z tej formy zaliczenia. Ocena końcowa z przedmiotu, w zależności od sumy uzyskanych punktów (maksymalnie 100 pkt) jest następująca (w nawiasach ocena wg skali ECTS):

- 0 – 50 pkt: niedostateczna (F),
- 51 – 60 pkt: dostateczna (E),
- 61 – 70 pkt: dostateczna plus (D),
- 71 – 80 pkt: dobra (C),
- 81 – 90 pkt: dobra plus (B),
- 91 – 100 pkt: bardzo dobra (A).

Bilans punktów ECTS:

Aktywność	Obciążenie studenta
Udział w wykładach	10 godz.
Udział w ćwiczeniach laboratoryjnych	18 godz.

Przygotowanie się do egzaminu	22 godz.
Przygotowanie się do ćwiczeń laboratoryjnych	23 godz.
Udział w konsultacjach z przedmiotu	2 godz.
Sumaryczne obciążenie pracą studenta	**75 godz.**
Punkty ECTS za przedmiot	**3 ECTS**