KARTA OPISU MODUŁU KSZTAŁCENIA

Nazwa modułu/przedmiotu	Kod
Kryptografia	**1010332511010331905**

Kierunek studiów	Profil kształcenia (ogólnoakademicki, praktyczny)	Rok / Semestr
Informatyka	**(brak)**	**1 / 1**
Ścieżka obieralności/specjalność	Przedmiot oferowany w języku:	Kurs (obligatoryjny/obieralny)
-	**polski**	**obligatoryjny**

Stopień studiów:	**Forma studiów** (stacjonarna/niestacjonarna)
II stopień	**stacjonarna**

Godziny	Liczba punktów
Wykłady: **30** Ćwiczenia: **-** Laboratoria: **15** Projekty/seminaria: **-**	**5**

Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny)	(ogólnouczelniany, z innego kierunku)
(brak)	**(brak)**

Obszar(y) kształcenia i dziedzina(y) nauki i sztuki	**Podział ECTS (liczba i %)**
nauki techniczne	**5 100%**

Odpowiedzialny za przedmiot / wykładowca:

dr inż. Anna Grocholewska-Czuryło
email: anna.grocholewska-czurylo@put.poznan.pl
tel. +48 61 665 37 57
Wydział Elektryczny
ul. Piotrowo 3A 60-965 Poznań

Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:

1	**Wiedza:**	Ma poszerzoną i pogłębioną wiedzę w zakresie wybranych zagadnień matematyki. Ma pogłębioną wiedzę w zakresie bezpieczeństwa danych.
2	**Umiejętności:**	Potrafi zaproponować i uzasadnić ulepszenia istniejących rozwiązań informatycznych.
3	**Kompetencje społeczne**	Potrafi myśleć i działać w sposób kreatywny i przedsiębiorczy.

Cel przedmiotu:

Celem jest nauczenie studentów zasad działania i projektowania algorytmów kryptograficznych.

Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia

Wiedza:

1. Ma pogłębioną wiedzę w zakresie kryptografii i wstępna z kryptoanalizy. - [K_W11]

Umiejętności:

1. Potrafi - przy formułowaniu i rozwiązywaniu problemów informatycznych - integrować wiedzę z różnych dziedzin i dyscyplin naukowych. - [K_U07]

Kompetencje społeczne:

1. Potrafi myśleć i działać w sposób kreatywny i przedsiębiorczy. - [K_K01]

Sposoby sprawdzenia efektów kształcenia

Wykład zaliczany jest na podstawie egzaminu pisemnego; kontynuacją egzaminu pisemnego może być egzamin ustny. Kryterium formalnym zdania egzaminu pisemnego jest uzyskanie więcej niż połowę maksymalnej liczby punktów zsumowanych za wszystkie uzyskane odpowiedzi.

Ćwiczenia laboratoryjne zalicza się na podstawie obecności, wykonanych ćwiczeń, jakości sprawozdań i sprawdzianu końcowego.

Treści programowe

Zastosowane metody kształcenia: wykład z prezentacją multimedialną, uzupełniany przykładami podawanymi na tablicy, teoria przedstawiana w ścisłym powiązaniu z praktyką.

Laboratoria- szczegółowe recenzowanie sprawozdań przez prowadzącego laboratoria i dyskusje nad komentarzami oraz eksperymenty obliczeniowe.

Wykłady obejmują:

Szyfry blokowe (przykłady budowy szyfrów blokowych; permutacje, podstawienia, funkcje boolowskie; kryteria projektowania bloków podstawień). Generatory ciągów pseudolosowych (generatory ciągów; komponenty generatorów: LFSR, NFSR, FCSR; losowość ciągów; złożoność liniowa ciągów). Szyfry strumieniowe (szyfry synchroniczne i samosynchronizujące; przykłady). Szyfry wykładnicze (Rabina, El-Gamala, Pohlinga-Hellmana, plecakowy). Funkcje skrótu (dedykowane (SHA); zbudowane z wykorzystaniem arytmetyki modularnej; atak urodzinowy). Podpisy cyfrowe (DSA; El-Gamala; kryptografia na krzywych eliptycznych). Uwierzytelnianie (dowody z wiedzą zerową). Niezaprzeczalność. Zarządzanie materiałem kryptograficznym (protokół

El-Gamala, współdzielenie sekretuł model Lenstry-Verheula).

Modyfikacja (wykład 2017) Algorytmy na krzywych eliptycznych.

Modyfikacja (laboratoria 2017): Kryptograficzne kryteria projektowania bloków podstawień ? testowanie S-bloków. Kryterium lawinowości SAC, Algorytm Berlecampa-Massey'a. Metody podziału sekretu. Szyfrowanie uwierzytelnione.

Literatura podstawowa:

1. Teoria bezpieczeństwa systemów komputerowych, Pieprzyk J., Hardjono T., Seberry J., Helion 2003

2. Kryptografia stosowana, Menezes A., Oorschot P., Vanstone S., WNT 2005

Literatura uzupełniająca:

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Wykłady	30
2. Bieżąca praca nad zagadnieniami przekazywanymi na wykładzie	15
3. Ćwiczenia laboratoryjne	15
4. Przygotowanie do laboratoriów	15
5. Przygotowanie do sprawdzianu	10
6. Przygotowanie sprawozdań z laboratorium	10
7. Przygotowanie do egzaminu	20
8. Udział w konsultacjach i egzaminie	10

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	125	5
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	50	2
Zajęcia o charakterze praktycznym	50	2