Nazwa przedmiotu							
Kryptografia praktyczna							
Practical cryptography							
Dyscyplina							Oznaczenie przedmiotu
Informatyka							
Rodzaj przedmiotu	Stopień studiów	Tryb studiów		Język zajęć		Rok	Semestr
Do wyboru	1	niestacjonarne		polski / angielski		IV	VII
Rodzaj zajęć		Wyk.	Ćw.	Lab.	Proj.	Sem.	Liczba punktów ECTS
Liczba godzin w semestrze		9	0	18	0	0	5
Koordynator	Dr Marek Matusiewicz mm@el.pcz.czest.pl						
Prowadzący	Dr Marek Matusiewicz mm@el.pcz.czest.pl Dr inż. Łukasz Piątek l_piatek@el.pcz.czest.pl Prof. Andriy Kityk kityk@el.pcz.czest.pl						

II. KARTA PRZEDMIOTU

Cel przedmiotu

C1. Nauczenie studenta podstawowych szyfrów z kluczem publicznym.

C2. Nauczenie studenta podstawowych szyfrów z kluczem tajnym.

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1. Programowanie w języku C#.
2. Algebra liniowa.
3. Matematyka dyskretna.

Efekty kształcenia

EK1. Student zna podstawowe algorytmy szyfrowania.
EK2. Student potrafi stosować algorytmy szyfrowania w praktyce.

Treści programowe: wykłady	Liczba godzin
W 1 – Podstawy teorii informacji, złożoność obliczeniowa algorytmu, arytmetyka modularna.	1
W 2 – Szyfry podstawieniowe, szyfry monoalfabetyczne, szyfry wieloalfabetowe.	1
W 3 – Szyfrująca maszyna rotorowa – ENIGMA, Szyfry poligramowe	1
W 4 – Podstawy szyfrowania wykładniczego. Algorytm DES.	1
W 5 – Algorytmy z kluczem jawnym: algorytm RSA.	1
W 6 – Funkcje skrótu.	1
W 7 – Algorytmy podpisu cyfrowego: algorytm podpisów cyfrowych DSA.	1
W 8 – Protokoły kryptograficzne. Wykrywanie łamania protokołu. Protokoły przesyłania informacji oraz protokoły wymiany i zarządzania kluczami.	1
W 9 – Zastosowanie kryptografii w bazach danych.	1
SUMA	**15**

Treści programowe: laboratorium	Liczba godzin
L 1 – Liczby pierwsze:Generator liczb pierwszych, Sito Eratostenesa. Liczby względnie pierwsze: algorytm Euklidesa, funkcja Eulera. Odwracanie wykładnika w zbiorze liczb naturalnych.	**3**
L 2 – Przygotowanie tekstu do szyfrowania: podział tekstu na znaki.	**1**
L 3 – Szyfry: szyfr przestawieniowy.	**1**
L 4 - Szyfry: szyfr Cezara.	**1**
L 5 – Szyfry: szyfr Playfaira.	**2**
L 6 – Szyfry: szyfr Vigenere'a.	**1**
L 7 – Kryptosystem RSA.	**2**
L 8 - Kryptosystem Hilla.	**2**
L 9 – Podpis cyfrowy asymetryczny – generowanie podpisu za pomocą szyfru RSA.	**2**
L 10 – System uzgadniania klucza Diffiego-Hellmana.	**1**
L 11 – Protokół podziału informacji pomiędzy n osobami.	**2**
SUMA	**18**

Narzędzia dydaktyczne

1. Wykład z prezentacją multimedialną.

2. Laboratorium komputerowe

Sposoby oceny efektów kształcenia (F – ocena Formująca, P – ocena Podsumowująca)

F1. Aktywność na wykładach (obecność,dyskusja).
P1. Zaliczenie na ocenę.
P2. Egzamin na ocenę.

Obciążenie pracą doktoranta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z prowadzącym	27
Zapoznanie się ze wskazaną literaturą	30
Przygotowanie do zajęć laboratoryjnych	33
Przygotowanie do egzaminu	35
Sumaryczna liczba godzin/punktów ECTS dla przedmiotu	**125 / 5 ECTS**

Wykaz literatury podstawowej i uzupełniającej

1. **Niels Ferguson, Bruce Shneier, Kryptografia w praktyce, Helion 2004.**
2. **Marek R. Ogiela, Podstawy kryptografii, AGH Uczelniane wydawnictwa Naukowo Dydaktyczne Kraków 2000**
3. **Friedrich L. Bauer, Sekrety kryptografii, Helion 2004**

Macierz realizacji efektów kształcenia

Efekt kształcenia	Odniesienie efektu do efektów kształcenia dla dyscypliny naukowej Elektrotechnika*	Cele przedmiotu	Forma zajęć	Narzędzia dydaktyczne	Sposób oceny
EK1	KINF1_W06	C1	W, Lab	1, 2	F1, P1,P2
EK2	KINF1_U12	C2	W, Lab	1, 2	F1, P1,P2

* – wg załącznika

II. FORMY OCENY – SZCZEGÓŁY

Ocena	Efekty
EK1	**Student zna podstawowe algorytmy szyfrowania.**
2	Student nie zna podstawowych algorytmow szyfrowania.
3	Student zna ogólną zasadę algorytmow symetryczych oraz niesymetrycznych..
3.5	Student zna szyfry podstawieniowe, szyfry monoalfabetyczne, szyfry wieloalfabetowe.
4	Student zna zasady budowania funkcji haszujących.
4.5	Student zna przynajmniej jeden algorytm asymetryczny.
5	Student zna kryptosystem RSA oraz ElGamala.
EK2	**Student potrafi stosować algorytmy szyfrowania w praktyce.**
2	Student nie potrafi zastosować żadnego szyfrowania.
3	Student potrafi zaszyfrować dane przynajmniej jednym algorytmem symetrycznym.
3.5	Student potrafi zaszyfrować i odszyfrować dane szyfrem Vigenere'a.
4	Student potrafi zbudować funkcję haszującą.
4.5	Student potrafi zaszyfrować dane przynajmniej jednym algorytmem asymetrycznym.
5	Student potrafi zbudować kryptosystem w oparciu RSA oraz ElGamala..

III. INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE

1. Wszelkie informacje dla studentów na temat planu zajęć dostępne są na tablicy ogłoszeń oraz na stronie el.pcz.pl.
2. Prowadzący udostępnia na pierwszych zajęciach treści wykładów.
3. Informacje na temat warunków zaliczania zajęć przekazywana jest studentom podczas pierwszych zajęć.