Nazwa przedmiotu							
Kryptografia							
Cryptography							
Dyscyplina							Oznaczenie przedmiotu
Elektrotechnika							9K_INS2
Rodzaj przedmiotu	Stopień studiów	Tryb studiów		Język zajęć		Rok	Semestr
obowiązkowy	2	niestacjonarne		polski / angielski		I	II
Rodzaj zajęć		Wyk.	Ćw.	Lab.	Proj.	Sem.	Liczba punktów ECTS
Liczba godzin w semestrze		18	0	18	0	0	6
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 –Arytmetyką modularna, chińskie zagadnienia resztowe, algorytmy wyznaczania logarytmów dyskretnych.	**1**
W 2 – Arytmetyka krzywych eliptycznych. Kongruencje kwadratowe i układy kongruencji kwadratowych.	**1**
W 3 – Kryptografia z kluczem tajnym.	**1**
W 4 - Zaawansowany standard szyfrowania danych DES/AES.	**2**
W 5 – Kryptosystemy hybrydowe	**1**
W 6 - Kryptosystemy oparte na logarytmach dyskretnych.	**1**
W 7 – Kryptosystem RSA z kluczem publicznym	**1**
W 8 - Kryptosystemy oparte na resztach kwadratowych.	**2**
W 9 - Kryptosystemy z kluczem publicznym oparte na krzywych eliptycznych.	**1**
W 10 – Podpisy cyfrowe	**1**
W 11 - Standard podpsu cyfrowego DSS	**2**
W 12 – Funkcje skrótu.	**1**
W 13 – Dzielenie sekretu	**1**
W 14 – Bezpieczeństwo w internecie oraz handlu w sieci	**1**
W 15 - Steganografia	**1**
SUMA	**18**

Treści programowe: laboratorium	Liczba godzin
L 1 – Generowanie dużych liczb pierwszych.	**1**
L 2 – Testy pierwszości	**2**
L 3 - Algorytmy wyznaczania logarytmów dyskretnych.	**2**
L 4 – Rozwiązywanie chińskich zagadnień resztowych.	**1**
L 5 – Rozwiązywanie kwadratowych zagadnień resztowych	**1**
L 6 – Arytmetyka krzywych eliptycznych.	**2**
L 7 – Generowanie funkcji skrótu.	**1**
L 8 – Problem dwóch wiadomości	**1**
L 9 – Kryptosystem RSA.	**3**
L 10 –Protokół wymiany klucza Diffiego-Hellman'a (RSAc.d.)	**1**
L 11 – Aspekty bezpieczeństwa RSA .	**1**

L 12 – Kryptosystem ElGamall'a	**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	36
Zapoznanie się ze wskazaną literaturą	34
Przygotowanie do zajęć laboratoryjnych	40
Przygotowanie do egzaminu	40
Sumaryczna liczba godzin/punktów ECTS dla przedmiotu	**150/ 6 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	KINF2_W09	C1	W, Lab	1, 2	F1, P1,P2
EK2	KINF2_U09	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 zasady funkcji skrótu.
4	Student zna kryptosystem RSA oraz ElGamala.
4.5	Student zna protokół wymiany klucza Diffiego-Hellman'a
5	Student zna standard podpsu cyfrowego.
EK2	**Student potrafi stosować algorytmy szyfrowania w praktyce.**
2	Student nie potrafi zastosować żadnego szyfrowania.
3	Student potrafi zaszyfrować dane przynajmniej jednym algorytmem z kluczem tajnym.
3.5	Student potrafi utworzyć funkcję skrótu.
4	Student potrafi zbudować kryptosystem w oparciu RSA oraz ElGamala.
4.5	Student potrafi zbudować system wymiany klucza Diffiego-Hellman'a
5	Student potrafi zbudować kryptosystem hybrydowy.

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.