KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Nazwa przedmiotu	Kod ECTS
Seminarium licencjackie: Algebraiczne aspekty kryptografii	11.1.0462

Nazwa jednostki prowadzącej przedmiot

null

Studia

wydział	kierunek		
Wydział Matematyki, Fizyki i Informatyki	Matematyka	poziom	pierwszego stopnia
		forma	stacjonarne
		moduł specjalnościowy	matematyka nauczycielska, matematyka ekonomiczna, matematyka
		specjalizacja	wszystkie

Nazwisko osoby prowadzącej (osób prowadzących)

dr Ewa Kozłowska-Walania

Formy zajęć, sposób ich realizacji i przypisana im liczba godzin

Formy zajęć

Seminarium

Sposób realizacji zajęć

zajęcia w sali dydaktycznej

Liczba godzin

Seminarium: 60 godz.

Liczba punktów ECTS

6

Cykl dydaktyczny

2017/2018 zimowy, 2017/2018 letni

Status przedmiotu

fakultatywny (do wyboru)

Język wykładowy

polski

Metody dydaktyczne

Analiza tekstów z dyskusją

Forma i sposób zaliczenia oraz podstawowe kryteria oceny lub wymagania egzaminacyjne

Sposób zaliczenia

- Zaliczenie na ocenę
- Zaliczenie (zal)

Formy zaliczenia

wykonanie pracy zaliczeniowej - projekt lub prezentacja

Podstawowe kryteria oceny

Sposób weryfikacji założonych efektów kształcenia

zakładany efekt kształcenia	Referat	Obserwacja postawy studenta na zajęciach	Aktywność w dyskusji	
	Wiedza			
K_W13	+			
K_W14	+			
	Umiejętności			
K_U15	+			
K_U16	+			
	Kompetencje			
K_K01		+		
K_K02			+	
K_K04		+		
K_K05	+			
K_K06	+			
K_K07		+		

Określenie przedmiotów wprowadzających wraz z wymogami wstępnymi

A. Wymagania formalne

B. Wymagania wstępne

Cele kształcenia

celem jest przygotowanie studentów do napisania pracy licencjackiej

Treści programowe

1. Elementy teorii liczb: oszacowanie czasu wykonywania działań arytmetycznych, kongruencje, algorytm Euklidesa, ułamki łańcuchowe, równanie Pella.
2. Pewne zagadnienia algebry: własności ciał skończonych, reszty kwadratowe i prawo wzajemności, pierścień wielomianów, tw. Hilberta o bazie i o zerach, bazy Gröbnera.
3. Podstawy kryptografii: szyfry afiniczne, macierze szyfrujące, systemy z kluczem publicznym, kryptosystem RSA, schemat Diffiego-Hellmana, zagadnienie logarytmu dyskretnego, dzielenie sekretów, problem pakowania plecaka.
4. Liczby pierwsze i rozkład na czynniki: liczby pseudopierwsze, metoda \rho, metoda Fermata, metoda sita kwadratowego.
5. Krzywe eliptyczne i hipereliptyczne: reguła dodawania, krzywe nad poszczególnymi ciałami, kryptosystemy eliptyczne i hipereliptyczne.

Wykaz literatury

1. Neal Koblitz, Algebraiczne aspekty kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2000.
2. Neal Koblitz, Wykład z teorii liczb i kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 1995.
3. Ian Blake, Gadiel Seroussi, Nigel Smart, Krzywe eliptyczne w kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.
4. Jerzy Gawinecki, Janusz Szmidt, Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii, Wojskowa Akademia Techniczna, Warszawa 1999.
5. Kenneth Ireland, Michael Rosen, A classical introduction to modern number theory, Springer-Verlag 1990.
6. Kenneth H. Rosen, Elementary number theory and its applications, Addison Wesley Publishing Company, 1988.
7. Yan Song Y., Teoria liczb w informatyce, PWN 2006.
8. Donald Knuth, Sztuka programowania, Wydawnictwo Naukowow-Techniczne, 2002.

Efekty kształcenia (obszarowe i kierunkowe)

Wiedza

Student

- nabywa doświadczenia w rozumieniu dowodów i osobistym dowodzeniu przez przedstawianie takich dowodów grupie.
- zdobywa wiedzę na temat uwarunkowań prawnych i etycznych w działalności naukowej. (K_W13)
- zdobywa wiedzę na temat prawa autorskiego i własności intelektualnej. (K_W14)

Umiejętności

Student

- umie przygotować wystąpienia ustne, potrafi przygotować referat i przeprowadzić jego prezentację na zadany temat, jest również w stanie przygotować odpowiednie teksty w formie pisemnej. (K_U15)
- nabywa umiejętności wyrażania treści matematycznych w mowie i w piśmie i

	potrafi określić swoje zainteresowania w matematycznych dyskusjach. (K_U16)
	Kompetencje społeczne (postawy)
	Student • potrafi samodzielnie wyszukiwać informacje w literaturze fachowej, przygotowując wystąpienia przed grupą. (K_K05) • aktywnie uczestniczy w seminarium i potrafi formułować pytania służące pogłębieniu własnego rozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania. (K_K02, K_K06) • zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia. (K_K01) • rozumie znaczenie uczciwości intelektualnej w działaniach własnych i innych osób. (K_K04) • potrafi myśleć i działać w sposób przedsiębiorczy. (K_K07)
Kontakt	
retrakt@math.univ.gda.pl	