**Nazwa przedmiotu:**

Obliczeniowa teoria liczb w informatyce i telekomunikacji

**Koordynator przedmiotu:**

Andrzej Paszkiewicz

**Status przedmiotu:**

Fakultatywny dowolnego wyboru

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Telekomunikacja

**Grupa przedmiotów:**

Przedmioty techniczne - zaawansowane

**Kod przedmiotu:**

OTL

**Semestr nominalny:**

7 / rok ak. 2018/2019

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

100

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

3

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

3

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład: | 30h |
| Ćwiczenia: | 15h |
| Laboratorium: | 0h |
| Projekt: | 15h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Brak

**Limit liczby studentów:**

48

**Cel przedmiotu:**

Zapoznanie studentów z metodami teorii liczb w odniesieniu do kryptografii, kodowania informacji, projektowania układów logicznych oraz obliczeń rozproszonych. Omawiane są metody i algorytmy teorii liczb, które znajdują ważne zastosowania w ramach współczesnej informatyki i telekomunikacji. Większość prezentowanych metod i algorytmów została opracowana w ciągu ostatnich lat i jest doskonalona w dalszym ciągu.

**Treści kształcenia:**

1. Liczby pierwsze, złożone, osobliwości rozkładu liczb pierwszych w zbiorze liczb naturalnych. Metody sita. Szybkie algorytmy wyznaczanie wartości funkcji zliczającej liczby pierwsze. Algorytmy Meissela, Lehmera, Odlyzki i Deleglise'a;
2. Operacje arytmetyczne na liczbach naturalnych. Reprezentacja długich liczb naturalnych. Pakiety do działań arytmetycznych na liczbach długich. Sprzętowa reprezentacja wielkich liczb naturalnych i działania na nich.
3. Klasyczne algorytmy generowania liczb pierwszych. Probabilistyczne i deterministyczne testy pierwszości. Testy typu p-1 i p+1, Ciągi Lucasa, liczby pseudopierwsze i silnie pseudopierwsze, liczby Carmichaela i ich rozkład;
4. Niereszty kwadratowe i ich rozmieszczenie. Kwadratowe prawo wzajemności. Zastosowanie niereszt kwadratowych w kryptografii silnych szyfrów strumieniowych;
5. Pierwiastki pierwotne a logarytm dyskretny. Zastosowanie pierwiastków pierwotnych w kodowaniu nadmiarowym. Rozkład asymptotyczny liczb pierwszych o zadanych najmniejszych pierwiastkach pierwotnych;
6. Arytmetyka modularna w rozszerzeniach arytmetycznych. Twierdzenie chińskie o resztach i jego zastosowania, ;
7. Indeks i logarytm dyskretny. Nowoczesne metody szybkiego wyznaczania logarytmu dyskretnego w ciałach skończonych prostych i rozszerzonych;
8. Algorytmy faktoryzacji liczb naturalnych i wielomianów pod w kontekście kryptoanalizy niektórych asymetrycznych systemów szyfrowania;
9. Arytmetyka krzywych eliptycznych. Szybkie działania arytmetyczne na krzywych eliptycznych realizowane programowo i sprzętowo.. Generowanie krzywych eliptycznych nadających się do kryptografii;
10. Arytmetyka krzywych eliptycznych i jej zastosowanie do do badania pierwszości (ECPP), test Kiliana-Goldwasser oraz Atkina Moraina;
11. Bazy wielomianowe i normalne jako jedna z koncepcji realizacji szybkich działań arytmetycznych w arytmetyce rozszerzonej. Optymalne bazy normalne. Wykorzystanie baz normalnych do efektywnej implementacji działań arytmetycznych z wykorzystaniem sprzętu;
12. Transformacje teorioliczbowe i ich wykorzystanie do szybkiego mnożenia modularnego.
13. Wielomiany nierozkładalne i pierwotne. Rozmnażanie wielomianów pierwotnych. Algorytmy wyszukiwania wielomianów nierozkładalnych oraz faktoryzacji.
14. Sieciowe projekty obliczeniowej teorii liczb (Projekt Cunninghama, GIMPS, wyznaczanie wartości funkcji );
15. Obliczeń rozproszone jako efektywna metoda projektowania skomplikowanych schematów szyfrowania oraz wyznaczania ich słabych punktów.

**Metody oceny:**

projekt, kolokwia cząstkowe, egzamin

**Egzamin:**

tak

**Literatura:**

1. M. Bressoud: Factorization and Primality Testing, Springer-Verlag, New York, Berlin, 1989;
2. H. Cohen: A Course in Computational and Algebraic Number Theory, Berlin, Heidelberg;
3. R. Crandall, C. Pomerance: Prime Numbers, A Computational Perspective, Springer-Verlag, New York, Berlin, 2001;
4. R. J. MCEliece, Finite Fields for Computer Scientists and Engineers, Kluwer Accad. Publ., Boston, 1987;
5. A. Paszkiewicz, A. Schinzel:: Numerical calcation of the density of prime numbers with a given least primitive root, Math. Comp. V. 71, No. 240, pp. 1781-1797, Nov. 2001;
6. A. Paszkiewicz, A. Schinzel: On the least prime primitive root modulo a prime, Math. Comp. V. 71, No. 239, pp. 1307-1321, Jan. 2002;
7. A. Paszkiewicz: Some observations concerning irreducible trinomials and pentanomials over, Tatra Mt. Math. Publ. 32 (2005), 129-142
8. A. Paszkiewicz: Przegląd Telekomunikacyjny Wiadomości Telekomunikacyjne, Cykl artykułów drukowanych w latach 2006-2011;
9. J. H. Silverman, The arithmetic of elliptic curves, Springer Verl. 1992

**Witryna www przedmiotu:**

www.zpt.tele.pw.edu.pl

**Uwagi:**

Brak

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka T2A\_W01:**

Znajomość metod teorii liczb i ich wykorzystania w telekomunikacji i informatyce, ze szczegolnym uwzględnieniem kryptografii i kodowania.

Weryfikacja:

kolokwia czastkowe, egzamin

**Powiązane charakterystyki kierunkowe:** K\_W01, K\_W03, K\_W05, K\_W07, K\_W10

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

### Profil ogólnoakademicki - umiejętności

**Charakterystyka T2A\_U01:**

Zastosować poznane metody praktycznie.

Weryfikacja:

ćwiczenia, projekt

**Powiązane charakterystyki kierunkowe:** K\_U01, K\_U05, K\_U06, K\_U09, K\_U13, K\_U14, K\_U15

**Powiązane charakterystyki obszarowe:** I.P7S\_UK, I.P7S\_UW, III.P7S\_UW.1.o, III.P7S\_UW.3.o, I.P7S\_UO, III.P7S\_UW.2.o, III.P7S\_UW.4.o

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka T2A-K01:**

potrafi współdziałać i pracować w grupie, potrafi stawiać hipotezy i je weryfikować, potrafi odpowiednio określać priorytety realizowanego zadania,

Weryfikacja:

ćwiczenia, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01

**Powiązane charakterystyki obszarowe:** I.P7S\_KO