KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Wstęp do kryptografii [S1MNT1>F-WdK]

Przedmiot

Kierunek studiów
Matematyka nowoczesnych technologii

Rok/Semestr
3/5

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
30

Laboratorium
0

Inne
0

Ćwiczenia
15

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr Anna Iwaszkiewicz-Rudoszańska
anna.iwaszkiewicz-rudoszanska@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student powinien mieć podstawową wiedzę z zakresu algebry i matematyki dyskretnej. Powinien także przeprowadzać poprawne wnioskowania logiczne i rozumieć konieczność poszerzania swoich kompetencji.

Cel przedmiotu

Celem przedmiotu jest zapoznanie z matematycznymi podstawami kryptografii oraz przedstawienie podstawowych algorytmów i praktycznych zastosowań kryptografii z kluczem publicznym.

Przedmiotowe efekty uczenia się

Wiedza:
• zna pojęcia i twierdzenia z teorii liczb wykorzystywane w omawianych algorytmach kryptograficznych [K_W01(P6S_WG)];
• wyjaśnia ideę kryptografii z kluczem publicznym, wskazuje przykłady takich kryptosystemów [K_W01(P6S_WG)].

Umiejętności:
• wykonuje obliczenia niezbędne do szyfrowania i deszyfrowania w omawianych systemach

kryptograficznych [K_U01(P6S_UW)];
• wykorzystuje twierdzenia z teorii liczb i algebry w analizie systemów kryptograficznych. Uzasadnia poprawności działania wybranych systemów kryptograficznych [K_U01(P6S_UW)];

Kompetencje społeczne:
• zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia [K_K02(P6S_KK)];
• ma świadomość ograniczeń współczesnej kryptografii [K_K01(P6S_KK)].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykłady: ocena wiedzy i umiejętności wykazanych na zaliczeniu pisemnym, składającym się z pięciu równo punktowanych pytań; zagadnienia udostępnione studentom co najmniej dwa tygodnie przed zaliczeniem;
próg zaliczeniowy 50%, każde 10% więcej to pół oceny w górę.
Ćwiczenia: umiejętności weryfikowane na postawie trzech krótkich, równo punktowanych sprawdzianów; do zaliczenia potrzeba w sumie 50% możliwych do zdobycia punktów; każde 10% punktów więcej to pół oceny w górę; możliwe dodatkowe punkty za rozwiązanie zadań domowych.

Treści programowe

Kryptografia - podstawowe pojęcia, historyczne sposoby szyfrowania, liczbowa reprezentacja tekstu szyfrowanego. Systemy z kluczem prywatnym i systemy z kluczem publicznym. Szyfry blokowe, szyfry strumieniowe. Logarytm dyskretny, protokół wymiany kluczy Diffiego-Hellmana, system ElGamala. Algorytmy dla problemu logarytmu dyskretnego. RSA. System Rabina. Podpisy cyfrowe. Krzywe eliptyczne, systemy kryptograficzne używające krzywych eliptycznych. Testy pierwszości i algorytmy faktoryzacji. Funkcje skrótu. Dzielenie sekretów, dowody o wiedzy zerowej, zobowiązanie bitowe. Kryptografia postkwantowa.

Tematyka zajęć

Aktualizacja: 22.05.2024r.
Wykłady:
• kryptografia - podstawowe pojęcia, historyczne sposoby szyfrowania (szyfr Cezara, Viegenere'a, Hilla);
• liczbowa reprezentacja tekstu szyfrowanego;
• systemy z kluczem prywatnym i systemy z kluczem publicznym;
• szyfry blokowe (AES, tryby działania szyfrów blokowych);
• szyfry strumieniowe;
• logarytm dyskretny (problem logarytmu dyskretnego w grupie $\Phi(p)$ i w dowolnej skończonej grupie cyklicznej);
• protokół wymiany kluczy Diffiego-Hellmana;
• system ElGamala w grupie $\Phi(p)$ i w grupie multiplikatywnej ciała skończonego Fpf;
• system ElGamala (algorytm generowania A, szyfrowania i deszyfrowania, dowód poprawności deszyfrowania, przykłady szyfrowania w $\Phi(p)$ i w grupie multiplikatywnej ciała Fpf;
• algorytmy dla problemu logarytmu dyskretnego (algorytm Shanksa, Pohliga-Hellmana, metoda obliczania indeksu);
• RSA (podstawy matematyczne: algorytm Euklidesa, kongruencje, twierdzenie Fermata i Eulera; algorytm generowania kluczy, szyfrowania i deszyfrowania, dowód poprawności deszyfrowania, przykłady, wymagania dotyczące klucza, przykłady ataków);
• system Rabina (podstawy matematyczne: twierdzenie chińskie o resztach, reszty i niereszty kwadratowe, symbol Legendre'a i Jacobiego, prawo wzajemności reszt kwadratowych Gaussa; algorytm generowania kluczy, szyfrowania i deszyfrowania, algorytm wyznaczania pierwiastków kwadratowych, przykłady, przykłady ataków);
• podpisy cyfrowe (schemat podpisu cyfrowego, podpis RSA, Rabina, ślepe podpisy, podpis ElGamala, kanał podprogowy, DSA);
• krzywe eliptyczne (krzywe eliptyczne nad dowolnymi ciałami, dodawanie punktów na krzywych eliptycznych, krzywe eliptyczne nad ciałami skończonymi, systemy kryptograficzne używające krzywych eliptycznych);
• testy pierwszości i algorytmy faktoryzacji (test Fermata, Solovaya-Strassena, Millera-Rabina, faktoryzacja liczb Mersenne'a i Fermata, metoda Fermata, Dixona i $\rho - 1$ Pollarda, ρ Pollarda);

• funkcje skrótu;
• inne zastosowanie kryptografii z kluczem publicznym (dzielenie sekretów, dowody o wiedzy zerowej, zobowiązanie bitowe);
• kryptografia postkwantowa (kraty całkowitoliczbowe, wymiana klucza oparta na LWE).
Ćwiczenia:
• historyczne sposoby szyfrowania;
• system ElGamala w grupie Φ(p) i w grupie multiplikatywnej ciała Fpf;
• algorytm Euklidesa, kongruencje, twierdzenie Fermata i Eulera;
• RSA;
• twierdzenie chińskie o resztach, reszty i niereszty kwadratowe, prawo wzajemności reszt kwadratowych Gaussa;
• system Rabina;
• działania na punktach krzywych eliptycznych, wyznaczanie punktów na krzywej eliptycznej nad ciałem skończonym;
• testy pierwszości, algorytmy faktoryzacji i algorytmy dla problemu logarytmu dyskretnego.

Metody dydaktyczne

Wykłady: prezentacja (zawartość prezentacji przekazywana studentom przed wykładem) uzupełniana dowodami i przykładami przedstawianymi na tablicy, z pytaniami kierowanymi do studentów; teoria przedstawiana w powiązaniu z aktualną wiedzą studentów.
Ćwiczenia: rozwiązywanie przykładowych zadań na tablicy, samodzielne rozwiązywanie zadań przez studentów, inicjowanie dyskusji nad rozwiązaniami, szczegółowe recenzowanie rozwiązań przez prowadzącego
ćwiczenia.

Literatura

Podstawowa:
• N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa 1995;
• A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2005;
• J.-P. Aumasson, Nowoczesna kryptografia, PWN, Warszawa 2018;
• D. Wong, Prawdziwy świat kryptografii, PWN, Warszawa 2023.

Uzupełniająca:
• D.R. Stinson, kryptografia w teorii i w praktyce, WNT, Warszawa 2005;
• W. Marzantowicz, P. Zarzycki, Elementarna teoria liczb, PWN, Warszawa 2006.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	75	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00