Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Podstawy kryptografii (P) , PG_00168371		
Kierunek studiów	Informatyka (P)		
Data rozpoczęcia studiów	październik 2024 r.	Rok akademicki realizacji przedmiotu	2026/2027
Poziom kształcenia	I stopnia - licencjackie	Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć fakultatywnych
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	3	Język wykładowy	polski
Semestr studiów	5	Liczba punktów ECTS	2.0
Profil kształcenia	praktyczny	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Rektor -> Wydział Matematyki, Fizyki i Informatyki -> Instytut Informatyki		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr Andrzej Borzyszkowski	
	Prowadzący zajęcia z przedmiotu		

Formy zajęć

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	15.0	0.0	15.0	0.0	0.0	30

W tym liczba godzin zajęć na odległość: 0.0

Aktywność studenta i liczba godzin pracy

Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
Liczba godzin pracy studenta	30	0.0	0.0	30

Cel przedmiotu

Przekazanie wiedzy na temat współczesnej kryptografii, zapoznanie się w praktyce z kilkoma najważniejszymi narzędziami używanymi w w/w.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[INFL3_K01] zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia	zdaje sobie sprawę z możliwych zagrożeń w kontekście używania komputerów i ma wiedzę na temat stosowanych rozwiązań rozumie, jakie są możliwości i jakie ograniczenia współczesnej kryptografii	[SK2] prezentacja/projekt/referat/ raport [SK4] test/egzamin - ustny lub pisemny
[INFL3_W02] ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie sztucznej inteligencji, języków formalnych, metod numerycznych	rozumie jak działa kryptografia asymetryczna, na czym polega podpis elektroniczny, jakie są metody badania integralności dokumentów, zna podstawowe algorytmy i protokoły kryptograficzne zna możliwe ataki na bezpieczeństwo systemów przetwarzania informacji	[SW4] test/egzamin - ustny lub pisemny [SW2] prezentacja/projekt/referat/ raport
[INFL3_U01] potrafi zastosować wiedzę matematyczną do formułowania, analizowania i rozwiązywania problemów związanych z informatyką, projektować i analizować algorytmy pod kątem ich poprawności i złożoności obliczeniowej	potrafi utworzyć bezpieczne hasło, utworzyć certyfikat X.509 lub PGP, obliczyć funkcję skrótu, napisać programy do szyfrowania i kryptoanalizy w różnych systemach kryptograficznych	[SU2] prezentacja/projekt/referat/ raport [SU4] test/egzamin - ustny lub pisemny

Treści przedmiotu

- Główne pojęcia, założenia kryptografii, kryptografia symetryczna i asymetryczna, klasyczne szyfry.
- Pojęcie doskonale bezpiecznego szyfru, szyfr jednorazowy, liczby losowe i pseudolosowe, szyfr strumieniowy.
- Funkcje i permutacje pseudolosowe. Szyfry blokowe i ich tryby.
- Integralność danych: MAC i funkcje skrótu, własności funkcji skrótu, atak urodzinowy. "Szyfruj, potem uwierzytelniaj".
- Kryptografia klucza prywatnego a kryptografia klucza publicznego. Idea kryptografii asymetrycznej, atak ze środka, uwierzytelnianie i podpis, szyfr hybrydowy.
- Implementacja kryptografii klucza publicznego: Teoria grup, twierdzenia Fermata, Eulera. Problemy trudne: problem rozkładu na czynniki, problem RSA, problem logarytmu dyskretnego, problem Diffie'go-Hellmana. RSA, system ElGamala.
- Schematy podpisu cyfrowego, w kryptografii symetrycznej i asymetrycznej, RSA, schemat ElGamala i DSS, użycie skrótu w podpisie. Infrastruktura klucza publicznego, X.509, PGP. Centra certyfikacji w Polsce. PGP w praktycznym działaniu.
- Elementy steganografii.

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
laboratorium	51.0%	60.0%
test końcowy	51.0%	40.0%

Zalecana lista lektur

Podstawowa lista lektur	materiały wykładowe na stronie WWW oraz portalu edukacyjnym
Uzupełniająca lista lektur	1. J. Katz, Y. Lindell, Introduction to modern cryptography, Chapman&Hall/CRC, 2008. 2. W. Trappe, L. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall , 2005. 3. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008
Adresy eZasobów	

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania

- Który/które z poniższych trybów szyfrów blokowych umożliwiają atakującemu niezauważoną manipulację kolejnością zaszyfrowanych bloków? (a) ECB (b) CTR (c) CBC (d) OFB
- Współczesna kryptografia klucza asymetrycznego jest przełomowym odkryciem ponieważ: (a) zapewnia radykalnie lepszą wydajność szyfrowania(b) umożliwia komunikację pomiędzy uczestnikami wcześniej nie kontaktującymi się (c) umożliwia implementację idei niezaprzeczalności autorstwa dokumentów (d) gwarantuje uwierzytelnianie uczestników
- Które z poniższych własności mają/powinny mieć funkcje skrótu: (a) jednoznaczność – nie ma dwóch dokumentów o tym samym skrócie (stosowane przy podpisie cyfrowym) (b) słaba bezkolizyjność – trudno zmodyfikować plik zachowując skrót (stosowane w kontroli integralności) (c) nieodwracalność – znając skrót trudno odtworzyć oryginalne dane (stosowane przy przechowywaniu haseł) (d) nieprzewidywalność – nawet mała zmiana powoduje dużą zmianę skrótu

Praktyki zawodowe w ramach przedmiotu

Nie dotyczy