Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Kryptografia i bezpieczeństwo systemów informatycznych (Z), PG_00179126		
Kierunek studiów	Informatyka (O)		
Data rozpoczęcia studiów	październik 2024 r.	Rok akademicki realizacji przedmiotu	2025/2026
Poziom kształcenia	I stopnia - licencjackie	Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć fakultatywnych
Forma studiów	niestacjonarne	Sposób realizacji	na uczelni
Rok studiów	2	Język wykładowy	polski
Semestr studiów	4	Liczba punktów ECTS	8.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	egzamin
Jednostka prowadząca			
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr Andrzej Borzyszkowski	
	Prowadzący zajęcia z przedmiotu	mgr Mateusz Miotk dr Andrzej Borzyszkowski	

Formy zajęć							
	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	30.0	0.0	0.0	60
	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	60	0.0	0.0	60

Cel przedmiotu	Zapoznanie z tematyką bezpieczeństwa systemów informatycznych ze szczególnym uwzględnieniem metod kryptograficznych. Poznanie terminologii w języku angielskim.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[INFL3_W02] posiada wiedzę w zakresie matematyki dyskretnej oraz metod probabilistycznych i statystyki	zdaje sobie sprawę z możliwych zagrożeń w kontekście używania komputerów i ma wiedzę na temat stosowanych rozwiązań, rozumie jak działa kryptografia asymetryczna, na czym polega podpis elektroniczny, jakie są metody badania integralności dokumentów, rozumie, jakie są możliwości i jakie ograniczenia współczesnej kryptografii. zna podstawowe algorytmy i protokoły kryptograficzne zna możliwe ataki na bezpieczeństwo systemów przetwarzania informacji	[SW4] test/egzamin - ustny lub pisemny [SW5] realizacja zadania problemowego
[INFL3_U09] potrafi oceniać przydatność paradygmatów i narzędzi programistycznych do rozwiązywania problemów różnego typu	potrafi ocenić prawną dopuszczalność różnych czynności związanych z łamaniem szyfrów	[SU4] test/egzamin - ustny lub pisemny
[INFL3_U03] potrafi projektować i analizować algorytmy pod kątem ich poprawności i złożoności obliczeniowej wykorzystując odpowiednie techniki algorytmiczne i struktury danych	potrafi utworzyć bezpieczne hasło, utworzyć certyfikat X.509 lub PGP, obliczyć funkcję skrótu, napisać programy do szyfrowania i kryptoanalizy w różnych systemach kryptograficznych	[SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego

Treści przedmiotu

- Główne pojęcia, założenia kryptografii, kryptografia symetryczna i asymetryczna, klasyczne szyfry.
- Pojęcie doskonale bezpiecznego szyfru, szyfr jednorazowy, liczby losowe i pseudolosowe.
- Bezpieczeństwo obliczeniowe szyfru, generatory pseudolosowe, szyfr strumieniowy, wielokrotne szyfrowanie, szyfry niedeterministyczne. Odporność na atak z wybranym tekstem jawnym, z wybranym kryptogramem.
- Funkcje i permutacje pseudolosowe. Szyfry blokowe i ich tryby. Szyfry blokowe w praktyce, DES, AES/ Rijndael.
- 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.
- Szyfr RSA, definicja, ataki, szyfr ElGamala, atak z wybranym kryptogramem, zobowiązanie bitowe. Schematy podpisu cyfrowego, w kryptografii symetrycznej i asymetrycznej, RSA i jego słabości, schemat ElGamala i DSS, użycie skrótu w podpisie. Infrastruktura klucza publicznego.
- Technologia blockchain.
- Klucze. Protokoły kryptograficzne, atak ze środka (man-in-the-middle), atak przez powtórzenie, liczby jednorazowe, znaczniki czasu, atak denial of-service, bilety, Kerberos.
- Elementy steganografii.

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
egzamin	51.0%	40.0%
laboratoria	51.0%	60.0%

Zalecana lista lektur

Podstawowa lista lektur	Andrzej Borzyszkowski, materiały do przedmiotu dostępne na stronie www.
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

1. Czy mała przestrzeń kluczy może zapewnić bezpieczeństwo szyfru? Czy duża przestrzeń kluczy jest gwarancją bezpieczeństwa. Uzasadnij.
2. Jakie znasz tryby pracy szyfrów blokowych? Omów pokrótce wady i zalety różnych trybów.
3. Podaj kilka różnic pomiędzy infrastrukturą klucza publicznego a modelem zaufania używanym w PGP.

Praktyki zawodowe w ramach przedmiotu

Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.