KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Nazwa przedmiotu	Kod ECTS
Podstawy kryptografii (P)	11.0.0222

Nazwa jednostki prowadzącej przedmiot

Instytut Informatyki

Studia

wydział	kierunek		
Wydział Matematyki, Fizyki i Informatyki	Informatyka	poziom	pierwszego stopnia
		forma	stacjonarne
		moduł specjalnościowy	wszystkie
		specjalizacja	wszystkie

Nazwisko osoby prowadzącej (osób prowadzących)

dr Andrzej Borzyszkowski

Formy zajęć, sposób ich realizacji i przypisana im liczba godzin

Formy zajęć

Wykład, Ćw. laboratoryjne

Sposób realizacji zajęć

zajęcia w sali dydaktycznej

Liczba godzin

Wykład: 15 godz., Ćw. laboratoryjne: 15 godz.

Liczba punktów ECTS

2
Przedmiot fakultatywny w wymiarze 15h wykładu i 15h laboratorium + praca własna studenta.

Termin realizacji przedmiotu

2022/2023 letni

Status przedmiotu

fakultatywny (do wyboru)

Język wykładowy

polski

Metody dydaktyczne

- Wykład z prezentacją multimedialną
- ćwiczenia laboratoryjne - przygotowanie programów związanych z kryptografią, zapoznanie się z istniejącymi rozwiązaniami

Forma i sposób zaliczenia oraz podstawowe kryteria oceny lub wymagania egzaminacyjne

Sposób zaliczenia

- Zaliczenie na ocenę
- Zaliczenie (zal)

Formy zaliczenia

- ustalenie oceny zaliczeniowej na podstawie ocen cząstkowych otrzymywanych w trakcie trwania semestru
- kolokwium

Podstawowe kryteria oceny

Ćwiczenia: systematyczna praca potwierdzająca umiejętności oraz wiedzę
Wykład: końcowy test pisemny

Sposób weryfikacji założonych efektów uczenia się

zakładany efekt kształcenia	egzamin	kolokwium	program	referat	raport	aktywność w dyskusji	obserwacja postawy
	Wiedza						
K_W02		X					
K_W03		X					
K_W09		X					
K_W10		X					
P_W1			X				
P_W2			X				
P_W3			X				
P_W4			X				
	Umiejętności						
K_U01			X				X
K_U02			X				
K_U04							X
K_U06			X			X	X
K_U07			X				
K_U10			X			X	
K_U11							X
P_U1			X				
P_U2							X
P_U3							X
P_U4							X
	Kompetencje						
K_K01							X
K_K03						X	
K_K04							X
P_K1			X				X
P_K2							X

Określenie przedmiotów wprowadzających wraz z wymogami wstępnymi

A. Wymagania formalne

brak

B. Wymagania wstępne

- Matematyka dyskretna
- umiejętność programowania w C i/lub C++, Java, C#, python lub inny język wysokiego poziomu

Cele kształcenia

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

Treści programowe

- 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.
- Teoria liczb: złożoność działań algebraicznych, arytmetyka modularna, twierdzenia Fermata, Eulera, chińskie o resztach. Problem rozkładu na czynniki, testy pierwszości, problem RSA, problem logarytmu dyskretnego i problem Diffie'go-Hellmana.
- 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.
- 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.

Wykaz literatury

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.

Kierunkowe efekty uczenia się

K_W02: posiada wiedzę w zakresie matematyki dyskretnej oraz metod probabilistycznych i statystyki
K_W03: ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie algorytmów i struktur danych, języków formalnych, teorii automatów i złożoności obliczeniowej
K_W09: ma podstawową wiedzę dotyczącą prawnych i społecznych aspektów informatyki, w tym odpowiedzialności zawodowej i etycznej, własności intelektualnej, prywatności, ryzyka i odpowiedzialności związanej z systemami informatycznymi
K_W10: zna podstawowe zasady bezpieczeństwa i higieny pracy w zawodzie informatyka
K_U01: potrafi zastosować wiedzę matematyczną do formułowania, analizowania i rozwiązywania problemów związanych z informatyką
K_U02: potrafi projektować i analizować algorytmy pod kątem ich poprawności i złożoności obliczeniowej wykorzystując odpowiednie techniki algorytmiczne i struktury danych
K_U04: potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania
K_U06: potrafi pozyskiwać informacje z literatury, Internetu oraz innych źródeł, integrować je, oceniać ich wiarygodność, dokonywać interpretacji oraz wyciągać wnioski i formułować opinie
K_U07: potrafi projektować, tworzyć, uruchamiać i testować programy przy wykorzystaniu dedykowanych narzędzi oraz adekwatnych wzorców
K_U10: potrafi oceniać przydatność paradygmatów i narzędzi programistycznych do rozwiązywania problemów różnego typu
K_U11: potrafi identyfikować prawne problemy z zakresu informatyki, samodzielnie wyszukiwać obowiązujące w danej kwestii przepisy, posługiwać się podstawową terminologią prawniczą
K_K01: zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego uczenia się
K_K03: potrafi i jest gotów formułować opinie na temat podstawowych zagadnień informatycznych
K_K04: rozumie i docenia znaczenie uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie

Wiedza

Student, który uzyska zaliczenie
ma wiedzę na temat współczesnych rozwiązań w zakresie kryptografii:
- P_W1 zna zasady kryptografii klasycznej (symetrycznej)
- P_W2 rozumie jak działa kryptografia asymetryczna,
- P_W3 rozumie na czym polega podpis elektroniczny,
- P_W4 wie jakie są metody badania integralności dokumentów,

- i rozumie ograniczenia współczesnej kryptografii.

Umiejętności

Student, który uzyska zaliczenie:
- P_U2 potrafi napisać program do szyfrowania oraz do kryptoanalizy w kilku systemach szyfrowania (K_U01, K_U02, K_U04, K_U06, K_U07, K_U10)
- P_U1 potrafi wygenerować i zainstalować certyfikat używając program OpenSSL,
- P_U2 potrafi posługować się programem PGP,
- P_U3 potrafi skontrolować integralność danych za pomocą funkcji skrótu,

Kompetencje społeczne (postawy)

Student, który uzyska zaliczenie:
- P_K1 potrafi formułować wymagania dotyczące kryptografii w różnych zastosowaniach informatyki (K_K03)
- P_K2 rozumie pojęcie prywatności i poufności i postępuje etycznie (K_K04)

- rozumie konieczność dalszego kształcenia się.

Kontakt

a.borzyszkowski@inf.ug.edu.pl