KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Nazwa przedmiotu

Podstawy kryptografii

Kod ECTS

11.0.0084

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

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

Liczba punktów ECTS

3
Przedmiot fakultatywny w wymiarze 30h wykładu i 30h laboratorium + praca własna studenta.

Cykl dydaktyczny

2017/2018 zimowy

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

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

Podstawowe kryteria oceny

Potwierdzone umiejętności oraz posiadanie wiedzy na temat objęty przedmiotem.

Sposób weryfikacji założonych efektów kształcenia

zakładany efekt kształcenia	egzamin	kolokwium	projekt	referat	raport	aktywność w dyskusji	obserwacja postawy studenta.
	Wiedza						
K_W01	x	x	x				
K_W02	x	x	x				
	Umiejętności						
K_U01			x				
K_U03			x				x
K_U05			x				
K_U06			x				
K_U13			x				
K_U17							
	Kompetencje						
K_K01	x	x	x				x
K_K04							x
K_K06	x						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

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.

Efekty kształcenia (obszarowe i kierunkowe)

K_W01
ma wiedzę w zakresie matematyki obejmującą podstawy analizy matematycznej, algebry, matematyki dyskretnej (elementy logiki i teorii mnogości, kombinatoryki i teorii grafów), metod probabilistycznych i statystyki , metod numerycznych

Wiedza

Student, który uzyska zaliczenie:
- ma wiedzę na temat współczesnych rozwiązań w zakresie kryptografii, rozumie jak działa kryptografia asymetryczna, na czym polega podpis elektroniczny, jakie są metody badania integralności dokumentów,
- zna istniejące rozwiązania kryptograficzne, rozumie, jakie są możliwości i jakie ograniczenia współczesnej kryptografii.

Umiejętności

K_W02
ma uporządkowaną, podbudowaną teoretycznie wiedzę ogólną w zakresie programowania, algorytmów i złożoności, architektury systemów komputerowych, systemów operacyjnych, technologii sieciowych, języków i paradygmatów programowania, baz danych, inżynierii oprogramowania, języków formalnych
K_U01
potrafi zastosować wiedzę matematyczną do formułowania, analizowania i rozwiązywania prostych zadań związanych z informatyką
K_U03
potrafi pracować indywidualnie i w zespole informatyków, w tym także potrafi zarządzać swoim czasem oraz podejmować zobowiązania i dotrzymywać terminów
K_U05
potrafi pisać, uruchamiać i testować programy w wybranym środowisku programistycznym
K_U06
projektuje, analizuje pod kątem poprawności i złożoności obliczeniowej oraz programuje algorytmy; wykorzystuje podstawowe techniki algorytmiczne i struktury danych
K_U13
potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami kompresji i szyfrowania danych
K_U17
potrafi ocenić, na podstawowym poziomie, przydatność metod i narzędzi informatycznych
K_K01
zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia
K_K04
rozumie i docenia znaczenie uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie
K_K06
potrafi formułować opinie na temat podstawowych zagadnień informatycznych

Student, który uzyska zaliczenie:
- potrafi wygenerować i zainstalować certyfikat, użyć programu PGP, skontrolować integralność danych za pomocą funkcji skrótu, posłużyć się programem OpenSSL,
- wykorzystuje istniejące rozwiązania kryptograficzne, certyfikaty, funkcje skrótu itd.

Kompetencje społeczne (postawy)

Student, który uzyska zaliczenie:
- potrafi formułować wymagania dotyczące kryptografii w różnych zastosowaniach informatyki,
- postępuje etycznie, rozumie pojęcie prywatności i poufności.
- rozumie konieczność dalszego kształcenia się.

Kontakt

a.borzyszkowski@inf.ug.edu.pl