



**KAPITAŁ LUDZKI**  
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez  
Unię Europejską w ramach  
Europejskiego Funduszu  
Społecznego

**UNIA EUROPEJSKA**  
EUROPEJSKI  
FUNDUSZ SPOŁECZNY



<b>Nazwa przedmiotu</b>		<b>Kod ECTS</b>	
Kryptografia i bezpieczeństwo systemów informatycznych		11.3.0213	
<b>Nazwa jednostki prowadzącej przedmiot</b>			
Instytut Informatyki			
<b>Studia</b>			
<b>wydział</b>	<b>kierunek</b>	<b>poziom</b>	<b>pierwszego stopnia</b>
Wydział Matematyki, Fizyki i Informatyki	Informatyka	<b>forma</b>	niestacjonarne (zaoczne)
		<b>moduł</b>	wszystkie
		<b>specjalnościowy</b>	wszystkie
		<b>specjalizacja</b>	wszystkie
<b>Nazwisko osoby prowadzącej (osób prowadzących)</b>			
dr Andrzej Borzyszkowski			
<b>Formy zajęć, sposób ich realizacji i przypisana im liczba godzin</b>		<b>Liczba punktów ECTS</b>	
<b>Formy zajęć</b>		8 Przedmiot fakultatywny w wymiarze 30h wykładu i 30h laboratorium + praca własna studenta.	
Wykład, Ćw. laboratoryjne			
<b>Sposób realizacji zajęć</b>			
zajęcia w sali dydaktycznej			
<b>Liczba godzin</b>			
Ćw. laboratoryjne: 30 godz., Wykład: 30 godz.			
<b>Cykl dydaktyczny</b>			
2017/2018 zimowy			
<b>Status przedmiotu</b>		<b>Język wykładowy</b>	
fakultatywny (do wyboru)		polski	
<b>Metody dydaktyczne</b>		<b>Forma i sposób zaliczenia oraz podstawowe kryteria oceny lub wymagania egzaminacyjne</b>	
<ul style="list-style-type: none"> <li>- Wykład z prezentacją multimedialną</li> <li>- ćwiczenia laboratoryjne - przygotowanie programów związanych z kryptografią, zapoznanie się z istniejącymi rozwiązaniami</li> </ul>		<b>Sposób zaliczenia</b>	
		<ul style="list-style-type: none"> <li>- Zaliczenie na ocenę</li> <li>- Egzamin</li> </ul>	
		<b>Formy zaliczenia</b>	
		<ul style="list-style-type: none"> <li>- egzamin ustny</li> <li>- ustalenie oceny zaliczeniowej na podstawie ocen cząstkowych otrzymywanych w trakcie trwania semestru</li> </ul>	
		<b>Podstawowe kryteria oceny</b>	
		Potwierdzone umiejętności oraz posiadanie wiedzy na temat objęty przedmiotem.	
<b>Sposób weryfikacji założonych efektów kształcenia</b>			

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				
K_W10	x	x					
K_W11	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 Java, C#, python

**Cele kształcenia**

Zapoznanie z tematyką bezpieczeństwa systemów komputerowych ze szczególnym uwzględnieniem metod kryptograficznych.

**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.
- 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 dyskretniej (elementy logiki i teorii mnogości, kombinatoryki i teorii grafów), metod probabilistycznych i statystyki, metod

**Wiedza**

Student, który uzyska zaliczenie:

- zdaje sobie sprawę z możliwych zagrożeń w kontekście używania komputerów
- 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.

<p>numerycznych</p> <p>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</p> <p>K_W10 ma wiedzę na temat technologii sieciowych, w tym podstawowych protokołów komunikacyjnych, bezpieczeństwa i budowy aplikacji sieciowych</p> <p>K_W11 ma podstawową wiedzę dotyczącą prawnych i społecznych aspektów informatyki, w tym odpowiedzialności zawodowej i etycznej, kodeksów etycznych, własności intelektualnej, prywatności i swobód obywatelskich, ryzyka i odpowiedzialności związanej z systemami informatycznymi, zna zasady netykiety, rozumie zagrożenia związane z przestępczością elektroniczną</p> <p>K_U01 potrafi zastosować wiedzę matematyczną do formułowania, analizowania i rozwiązywania prostych zadań związanych z informatyką</p> <p>K_U03 potrafi pracować indywidualnie i w zespole informatyków, w tym także potrafi zarządzać swoim czasem oraz podejmować zobowiązania i dotrzymywać terminów</p> <p>K_U05 potrafi pisać, uruchamiać i testować programy w wybranym środowisku programistycznym</p> <p>K_U06 projektuje, analizuje pod kątem poprawności i złożoności obliczeniowej oraz programuje algorytmy; wykorzystuje podstawowe techniki algorytmiczne i struktury danych</p> <p>K_U13 potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami kompresji i szyfrowania danych</p> <p>K_U17 potrafi ocenić, na podstawowym poziomie, przydatność metod i narzędzi informatycznych</p> <p>K_K01 zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia</p> <p>K_K04 rozumie i docenia znaczenie uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie</p> <p>K_K06 potrafi formułować opinie na temat podstawowych zagadnień informatycznych</p>	<p><b>Umiejętności</b></p> <p>Student, który uzyska zaliczenie:</p> <ul style="list-style-type: none"> <li>- potrafi wygenerować i zainstalować certyfikat, użyć programu PGP, skontrolować integralność danych za pomocą funkcji skrótu, posłużyć się programem OpenSSL,</li> <li>- wykorzystuje istniejące rozwiązania kryptograficzne, certyfikaty, funkcje skrótu itd.</li> </ul>
	<p><b>Kompetencje społeczne (postawy)</b></p> <p>Student, który uzyska zaliczenie:</p> <ul style="list-style-type: none"> <li>- potrafi formułować wymagania dotyczące kryptografii w różnych zastosowaniach informatyki,</li> <li>- postępuje etycznie, rozumie pojęcie prywatności i poufności.</li> <li>- rozumie konieczność dalszego kształcenia się.</li> </ul>

## Kontakt

[a.borzyszkowski@inf.ug.edu.pl](mailto:a.borzyszkowski@inf.ug.edu.pl)