


**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>	
Podstawy kryptografii (P)		11.0.0222	
<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	forma	stacjonarne
		moduł	wszystkie
		specjalnościowy	wszystkie
		specjalizacja	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>		2 Przedmiot fakultatywny w wymiarze 15h wykładu i 15h laboratorium + praca własna studenta.	
Wykład, Ćw. laboratoryjne			
<b>Sposób realizacji zajęć</b>			
zajęcia w sali dydaktycznej			
<b>Liczba godzin</b>			
Wykład: 15 godz., Ćw. laboratoryjne: 15 godz.			
<b>Termin realizacji przedmiotu</b>			
2023/2024 letni			
<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>- Zaliczenie (zał)</li> </ul>	
		<b>Formy zaliczenia</b>	
		<ul style="list-style-type: none"> <li>- ustalenie oceny zaliczeniowej na podstawie ocen cząstkowych otrzymywanych w trakcie trwania semestru</li> <li>- kolokwium</li> </ul>	
		<b>Podstawowe kryteria oceny</b>	
		Ćwiczenia: systematyczna praca potwierdzająca umiejętności oraz wiedzę Wykład: końcowy test pisemny	
<b>Sposób weryfikacji założonych efektów uczenia się</b>			

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 posługiwać 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