

	Nazwa modułu. Blok przedmiotów wybieralnych						Kod modułu: M23
Wypełnia Zespól Kierunku	Nazwa przedmiotu: Bezpieczeństwo i ochrona danych						Kod przedmiotu:
	Nazwa jednostki prowadzącej przedmiot / moduł: INSTYTUT INFORMATYKI STOSOWANEJ						
	Nazwa kierunku: INFORMATYKA						
	Forma studiów: niestacjonarne			Profil kształcenia: PRAKTYCZNY		Specjalność: Projektowanie baz danych i oprogramowanie użytkowe	
	Rok / semestr: 4/7			Status przedmiotu /modułu: obowiązkowy		Język przedmiotu / modułu: polski	
	Forma zajęć	wykład	ćwiczenia	ćwiczenia laboratoryjne	konwersatorium	seminarium	inne (wpisać jakie)
	Wymiar zajęć	15		15			
	Koordynator przedmiotu / modułu		dr hab. inż. Zenon Ulman				
Prowadzący zajęcia		dr hab. inż. Zenon Ulman, dr inż. Robert Smyk					
Cel przedmiotu / modułu		Zapoznanie z podstawowymi zagrożeniami dla bezpieczeństwa baz danych. Zapoznajnie z polityką bezpieczeństwa, sposobami zabezpieczania sprzętu, różnymi aspektami ochrony danych, procedurami używania kluczy kryptograficznych, przepisami związanymi z ochrona systemów informatycznych, podstawami kryptografii oraz popularnymi algorytmami kryptograficznymi.					
Wymagania wstępne		Otwarta głowa, chęć do nauki i trochę matematyki.					
EFEKTY KSZTAŁCENIA						Odniesienie do efektów dla programu	
Nr	Wiedza						
01	Opanowuje elementy teorii liczb, arytmetyki modularnej i algebry abstrakcyjnej w celu samodzielnego projektowania standardowych algorytmów kryptograficznych.					K_W01, K_W12	
02	Zna podstawowe algorytmy kryptograficzne symetryczne i niesymetryczne					K_W06, K_W12	
03	Rozumie politykę bezpieczeństwa i zna źródła zagrożeń tego bezpieczeństwa					K_W17	
04	Zna podstawowe zasady pośrednie i bezpośrednie ochrony baz danych					K_W05, K_W08, K_W16	
	Umiejętności						
05	Potrafi zaprojektować podstawowe systemy kryptograficzne i je używać					K_U02, K_U07, K_U10	
06	Umie opracować bazę danych dla użytkowników o zróżnicowanych prawach dostępu					K_U10	
07	Potrafi samodzielnie analizować nowe sposoby zabezpieczenia danych					K_U10	
	Kompetencje społeczne						
08	Docenia wagę bezpieczeństwa informacji w bazach danych					K_K02	
09	Umie wyjaśnić zagadnienia pośredniej i bezpośredniej ochrony informacji.					K_K06	
TREŚCI PROGRAMOWE							
Forma zajęć – WYKŁAD							
Pośrednie sposoby ochrony danych							
<ol style="list-style-type: none"> 1. Polityka ochrony informacji w firmie 2. Aspekty i zasady ochrony baz danych 3. Śluz bezpieczeństwa i inne środki 4. Zasady stosowania środków ochrony, ochrona w internecie 5. Hakerzy i krakerzy – skutki działania 6. Źródła informacji o naruszeniu bezpieczeństwa i metody reagowania 							
Bezpośrednie sposoby ochrony danych							
<ol style="list-style-type: none"> 1. Podstawy kryptografii 2. Liczby pierwsze i podstawy teorii liczb i algebry abstrakcyjnej 3. arytmetyka modularna 							

4. Algorytmy kryptograficzne symetryczne DES, IDEA, Rijandel
5. Algorytmy niesymetryczne RSA
6. Protokoły kryptograficzne
7. Chińskie Twierdzenie o Resztach i jego użycie do ochrony baz danych

Sposoby podejścia do złamania szyfru

Forma zajęć – LABORATORIUM

1. Korzystanie z bibliotek kryptograficznych w wybranych platformach
2. Implementacja wybranych funkcji skrótu
3. Projektowanie algorytmu RSA i podpisu cyfrowego z jego użyciem
4. Użycie wybranych algorytmów strumieniowych
5. Praktyczne wykorzystanie pakietu kryptograficznego OpenSSL
6. Użycie Chińskiego Twierdzenia o Resztach do ochrony baz danych
7. Ćwiczenia z określeniem notacji O i złożoności obliczeniowej
8. Obliczenie NWD na podstawie algorytmu Euklidesa
9. Obliczenie inwersji multiplikatywnej modulo z użyciem rozszerzonego algorytmu Euklidesa

Metody kształcenia	Wykład, ćwiczenia częściowo audytoryjne i częściowo laboratoryjne.	
Metody weryfikacji efektów kształcenia		Nr efektu kształcenia z sylabusu
Sprawdziany z części teoretycznej i praktycznej		1 - 9
Projekt		5, 6, 7
Dyskusja		8, 9
Forma i warunki zaliczenia	2 kolokwia z wykładu, zaliczenie laboratorium	
Literatura podstawowa	<ol style="list-style-type: none"> 1. M. Konkowski: Podstawy kryptografii, Helion 2006 2. M. Kutyłkowski, W. B. Strothmann: Kryptografia – teoria i praktyka zabezpieczania systemów komputerowych, Oficyna wydawnicza ReadME, Warszawa 1999 3. R. Andersen: Inżynieria zabezpieczeń, WNT 4. D. Pipkin: Bezpieczeństwo informacji, WNT 	
Literatura uzupełniająca	<ol style="list-style-type: none"> 1. K. Mundia, Ch. Prossie: Hakerom śmierć, Wydawnictwo RM 2. F.L. Bauer, S. Lloyd: Podpis elektroniczny, klucz publiczny, Robomatic, Wrocław 2002 	
NAKŁAD PRACY STUDENTA:		
	Liczba godzin	
Udział w wykładach	15	
Samodzielne studiowanie tematyki wykładów	10	
Udział w ćwiczeniach audytoryjnych i laboratoryjnych*	15	
Samodzielne przygotowywanie się do ćwiczeń*	15	
Przygotowanie projektu / eseju / itp.*	15	
Przygotowanie się do egzaminu / zaliczenia	5	
Udział w konsultacjach	5	
Inne		
ŁĄCZNY nakład pracy studenta w godz.	80	
Liczba punktów ECTS za przedmiot	3 ECTS	
Obciążenie studenta związane z zajęciami praktycznymi*	45 1,8 ECTS	
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	35 1,4 ECTS	