

KARTA PRZEDMIOTU

1. Informacje ogólne

Nazwa przedmiotu i kod (wg planu studiów):	Architektura klucza PKI, D1_14
Nazwa przedmiotu (j. ang.):	Architekture PKI key
Kierunek studiów:	Informatyka
Specjalność/specjalizacja:	Bezpieczeństwo systemów informatycznych
Poziom kształcenia:	studia I stopnia
Profil kształcenia:	praktyczny (P)
Forma studiów:	studia stacjonarne
Obszar kształcenia:	nauki techniczne (wg wykazu)
Dziedzina:	nauki techniczne (wg wykazu)
Dyscyplina nauki:	informatyka
Koordinator przedmiotu:	mgr Radosław Gołąb

2. Ogólna charakterystyka przedmiotu

Przynależność do modułu:	kształcenia specjalnościowego/specjalizacyjnego
Status przedmiotu:	Obowiązkowy
Język wykładowy:	Polski
Rok studiów, semestr:	III, 6
Forma i wymiar zajęć według planu studiów:	stacjonarne - wykład 30 h, ćw. laboratoryjne 30 h
Interesariusze i instytucje partnerskie (nieobowiązkowe)	
Wymagania wstępne:	Analiza matematyczna, Algebra liniowa, Systemy operacyjne, Sieci komputerowe, Programowanie II,

3. Bilans punktów ECTS

Całkowita liczba punktów ECTS	4 (A + B)	stacjonarne
A. Liczba godzin wymagających bezpośredniego udziału nauczyciela z podziałem na typy zajęć oraz całkowita liczba punktów ECTS osiągniętych na tych zajęciach	Obecność na wykładach Obecność na ćwiczeniach laboratoryjnych W sumie: ECTS	30 30 60 2
B. Poszczególne typy zadań do samokształcenia studenta (niewymagających bezpośredniego udziału nauczyciela) wraz z planowaną średnią liczbą godzin na każde i sumaryczną liczbą ECTS	przygotowanie do zajęć uzupełnienie/studiowanie notatek przygotowanie do kolokwium studiowanie zalecanej literatury w sumie: ECTS	30 5 15 10 60 2
C. Liczba godzin praktycznych/laboratoryjnych w ramach przedmiotu oraz związana z tym liczba punktów ECTS	udział w ćwiczeniach laboratoryjnych praca praktyczna samodzielna w sumie: ECTS	30 60 90 3

4. Opis przedmiotu

<p>Cel przedmiotu: Celem przedmiotu jest zapoznanie studentów z podstawami systemów kryptograficznych oraz architekturą klucza PKI</p>
<p>Metody dydaktyczne: wykład, ćwiczenia projektowe</p>
<p>Treści kształcenia:</p> <p>Wykłady:</p> <ol style="list-style-type: none"> 1. Wstęp do kryptografii. Historia kryptografii. 2. Elementy algebry: teoria grup, ciała skończone. 3. Szyfrowanie symetryczne. 4. Szyfrowanie asymetryczne 5. Uwierzytelnianie. 6. Kryptografia klucza publicznego. Podpis cyfrowy. 7. Przegląd ataków kryptograficznych. <p>Ćwiczenia laboratoryjne:</p> <ol style="list-style-type: none"> 1. Praktyczne wykorzystanie wybranego narzędzia kryptograficznego 2. Instalacja i konfiguracja w środowisku laboratoryjnym, 3. Szyfrowanie nośników wymiennych, urządzeń mobilnych, 4. Zarządzanie kluczami.

5. Efekty kształcenia i sposoby weryfikacji

Efekty kształcenia K_W09, K_U01, K_U15, K_U16, K_K01, K_K03, K_K09				
Efekt przedmiotu (kod przedmiotu + kod efektu kształcenia)	Student, który zaliczył przedmiot (spełnił minimum wymagań)			Efekt kierunkowy
D1_14_K_W09	Wiedza: 1. Ma podstawową wiedzę nt. kodeksów etycznych dotyczących informatyki, zna zasady netykiety, rozumie zagrożenia związane z przestępczością elektroniczną, rozumie specyfikę systemów krytycznych ze względu na bezpieczeństwo			K_W09
D1_14_K_U01	Umiejętności: 1. Potrafi wykorzystać nabytą wiedzę matematyczną do opisu procesów, tworzenia modeli, zapisu algorytmów oraz innych działań w obszarze informatyki. 2. Ma umiejętność projektowania prostych sieci komputerowych; potrafi pełnić funkcję administratora sieci komputerowej oraz zapewnienia jej bezpieczeństwa. 3. Potrafi zabezpieczyć system informatyczny, serwer, aplikację, przesyłane dane przed nieuprawnionym dostępem, a także zapewnia bezpieczeństwo działania aplikacji.			K_U01
D1_14_K_U15				K_U15
D1_14_K_U16				K_U16
D1_14_K_K01	Kompetencje społeczne: 1. Rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe. 2. Zna przykłady i rozumie przyczyny wadliwie działających systemów informatycznych, które doprowadziły do poważnych strat finansowych, społecznych lub też do poważnej utraty zdrowia, a nawet życia. 3. Rozumie potrzebę zachowań profesjonalnych i przestrzegania zasad etyki, w tym uczciwości.			K_K01
D1_14_K_K03				K_K03
D1_14_K_K09				K_K09
Sposoby weryfikacji efektów kształcenia:				
Lp.	Efekt przedmiotu	Sposób weryfikacji	Ocena formująca – przykładowe sposoby jej wystawienia poniżej	Ocena końcowa przykładowe sposoby jej wystawienia poniżej
1	D1_14_K_W09	Aktywność podczas zajęć, rozwiązywanie zadań problemowych na zajęciach laboratoryjnych, test sprawdzający	sprawdzian wiedzy i umiejętności polegający na rozwiązaniu wskazanych przez prowadzącego zadań, test końcowy	Średnia z ocen formujących,
2	D1_14_K_U01 D1_14_K_U15 D1_14_K_U16	Aktywność podczas zajęć, rozwiązywanie zadań problemowych na zajęciach laboratoryjnych, test sprawdzający.	sprawdzian wiedzy i umiejętności polegający na rozwiązaniu wskazanych przez prowadzącego za-	Średnia z ocen formujących,

			dań, test końcowy	
3	D1_14_K_K01 D1_14_K_K03 D1_14_K_K09	Aktywność podczas zajęć, rozwiązywanie zadań problemowych na zajęciach laboratoryjnych, test sprawdzający.	sprawdzian wiedzy i umiejętności polegający na rozwiązaniu wskazanych przez prowadzącego zadań, test końcowy	Średnia z ocen formujących,
Kryteria oceny:				
w zakresie wiedzy				Efekt kształcenia
Na ocenę 3,0	Student uzyskał minimum 50% wymaganej wiedzy w zakresie obowiązującego materiału			D1_14_K_W09
Na ocenę 5,0	Student uzyskał minimum 90% wymaganej wiedzy w zakresie obowiązującego materiału			D1_14_K_W09
w zakresie umiejętności				
Na ocenę 3,0	Student uzyskał minimum 50% wymaganej wiedzy w zakresie obowiązującego materiału			D1_14_K_U01 D1_14_K_U15 D1_14_K_U16
Na ocenę 5,0	Student uzyskał minimum 90% wymaganej wiedzy w zakresie obowiązującego materiału			D1_14_K_U01 D1_14_K_U15 D1_14_K_U16
w zakresie kompetencji społecznych				
Na ocenę 3,0	Student uzyskał minimum 50% wymaganej wiedzy w zakresie obowiązującego materiału			D1_14_K_K01 D1_14_K_K03 D1_14_K_K09
Na ocenę 5,0	Student uzyskał minimum 90% wymaganej wiedzy w zakresie obowiązującego materiału			D1_14_K_K01 D1_14_K_K03 D1_14_K_K09
Kryteria oceny końcowej: samodzielne wykonanie ćwiczeń laboratoryjnych: 40%, aktywność za zajęciami: 20%, wynik testu sprawdzającego: 40%				
Zalecana literatura:				
<ol style="list-style-type: none"> 1. Stallings W., Ochrona danych w sieci i intersieci, WNT, Warszawa, 1997 2. Karbowski M., Podstawy kryptografii, Helion, Gliwice, 2014 3. Kaeo M., Tworzenie bezpiecznych sieci, Mikom, Warszawa, 2000 4. Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, Wydawnictwo Naukowe PWN, Warszawa, 2008 5. IT Professional, PRESSCOM Sp. z o.o., Wrocław 6. IT w Administracji, PRESSCOM Sp. z o.o., Wrocław 				

Informacje dodatkowe:

Dodatkowe obowiązki prowadzącego wraz z szacowaną całkowitą liczbą godzin:
Przygotowanie do wykładów i ćwiczeń laboratoryjnych – 60 godzin
Konsultacje – 15 godzin
Przygotowanie i poprawa testu – 5 godzin

W sumie: 80 godzin