UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Kryptografia

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Technologie informatyczne	**Cykl dydaktyczny** 2024/25
Specjalność -	**Kod zajęć** 17TINS.310N.00997.24
Jednostka organizacyjna Nadnotecki Instytut UAM w Pile	**Języki wykładowe** Polski
Poziom studiów studia inżynierskie pierwszego stopnia	**Obligatoryjność** Fakultatywny specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty nieprzypisane
Profil studiów profil praktyczny	

Koordynator zajęć	Marcin Gogolewski
Prowadzący zajęcia	Marcin Gogolewski

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 5	• Wykład: 30, Egzamin • Laboratorium: 30, Zaliczenie z oceną	5

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z algorytmami i protokołami zabezpieczania danych, konfiguracji oraz wykorzystania istniejących systemów.
C2	Przekazanie zasad z zakresu bezpieczeństwa (hasła, autoryzacja, blockchain).

Wymagania wstępne

Student powinien posiadać podstawową wiedzę z algorytmów, teorii liczb i algebry, programowania oraz obsługi systemu oparacyjnego.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	rozróżnia kryptografię symetryczną i asymetryczną, potrafi podać przykłady.	TIN_K3_W01, TIN_K3_W03_inz, TIN_K3_W10_inz	Egzamin pisemny
W2	wie co to funkcja haszująca, rozumie problemy związane z projektowaniem dobrych funkcji haszujących oraz potrafi podać przykłady.	TIN_K3_W02_inz, TIN_K3_W10_inz	Egzamin pisemny, Projekt
W3	zna przykłady historycznych algorytmów szyfrujących i powody, dla których nie są bezpieczne (w wybranych przypadkach potrafi podać metodę złamania).	TIN_K3_W10_inz	Egzamin pisemny, Projekt
W4	rozumie działanie protokołu TLS, systemu certyfikacji i weryfikacji ważności certyfikatów przez przeglądarkę internetową.	TIN_K3_W10_inz	Egzamin pisemny
W5	Rozumie ideę end-to-end encryption.	TIN_K3_W10_inz	Egzamin pisemny
W6	Zna ideę ataków Men in the Middle i sposoby zabezpieczeń.	TIN_K3_W10_inz, TIN_K3_W17	Egzamin pisemny
W7	zna przykłady algorytmów strumieniowych i blokowych oraz rozumie problemy związane z szyfrowaniem dłuższych bloków danych i zna podstawowe tryby szyfrowania (np. ECB, CBC,..).	TIN_K3_W01, TIN_K3_W05_inz, TIN_K3_W06_inz, TIN_K3_W10_inz	Egzamin pisemny, Projekt
Umiejętności – Student/ka:			
U1	potrafi wygenerować certyfikat dla domeny internetowej (z wykorzystaniem openssl lub analogicznych narzędzi).	TIN_K3_U01, TIN_K3_U14_inz	Projekt
U2	potrafi wygenerować parę kluczy do szyfrowania komunikacji (np. GPG).	TIN_K3_U14_inz	Projekt
Kompetencji społecznych – Student/ka:			
K1	rozumie konieczność zapewnienia bezpieczeństwa i prywatności komunikacji oraz potrafi przedstawić argumenty za stosowaniem silnych haseł, sprawdzonych algorytmów szyfrowania, czy autoryzacji dwuetapowej.	TIN_K3_K01, TIN_K3_K02, TIN_K3_K03, TIN_K3_K04, TIN_K3_K08	Egzamin pisemny, Projekt

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Algorytmy historyczne wraz z metodami kryptoanalizy, podstawy współczesnej kryptografii.	W3	Wykład, Laboratorium

2.	Podstawy funkcji haszujących, zastosowania (elektroniczny notariusz, bitcoin, przechowywanie haseł), ataki na funkcje haszujące.	W2	Wykład, Laboratorium
3.	Kryptografia symetryczna i asymetryczna, przykłady algorytmów asymetrycznych, problemy na których opiera się bezpieczeństwo, zastosowania.	W1, W7	Wykład, Laboratorium
4.	Kryptografia symetryczna, przykładowe algorytmy, standardy, metody przechowywania i generowania kluczy, tryby szyfrowania.	W1, W7, K1	Wykład, Laboratorium
5.	Komunikacja pomiędzy użytkownikami, End to End Encryption, protokoły bezpiecznej wymiany klucza.	W1, W5, W6, U2	Wykład, Laboratorium
6.	Protokół TLS, działanie, zasady, generowanie certyfikatów, CRL.	W4, W6, U1	Wykład, Laboratorium
7.	Losowość i pseudolosowość, generator LFSR i jego kryptoanaliza, shrinking LFSR, algorytm A5, algorytm BBS, obliczanie pierwiastka a problem faktoryzacji w kontekście BBS	W1, W2, U1, U2	Wykład, Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień
Laboratorium	Dyskusja, Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda projektu, Metoda aktywizująca - "burza mózgów", Praca w grupach, Rozwiązywanie zadań praktycznych

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Zdobycie powyżej 50% punktów z zadań na egzaminie - ocena 3.0 (co 10% + 0.5 oceny)
Laboratorium	Zdobycie powyżej 50% punktów z zadań w ramach ćwiczeń - ocena 3.0 (co 10% + 0.5 oceny)

Literatura

Obowiązkowa

1. "Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych" Mirosław Kutyłowski, Willy-B. Strothmann Wydawnictwo READ ME, ISBN 83-7147-087-8

Dodatkowa

1. A.J.Menezes, P.C van Oorschot, S.A.Vanstone , Handbook of Applied Cryptography, CRC, 1996, ISBN 0-8493-8523-7
2. D.R.Stinson , Cryptography. Theory and Practice, CRC Press, 1995, ISBN 0-8493-8521-0
3. N.Koblitz , Algebraiczne aspekty kryptografii, WNT, 2000, ISBN ISBN 83-204-2418-6.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	30

Laboratorium	30
Czytanie wskazanej literatury	10
Przygotowanie raportu	20
Przygotowanie projektu	30
Przygotowanie do zajęć	10
Przygotowanie do egzaminu	20
Łączny nakład pracy studenta	**Liczba godzin** 150
Liczba punktów ECTS	**ECTS** 5

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
TIN_K3_K01	Absolwent/ka jest gotów/gotowa do zrozumienia wagi i znaczenia matematyki w rozmaitych zastosowaniach, w szczególności w informatyce
TIN_K3_K02	Absolwent/ka jest gotów/gotowa do zrozumienia roli informatyki w kształtowaniu życia społecznego
TIN_K3_K03	Absolwent/ka jest gotów/gotowa do zaakceptowania odpowiedzialności zawodowej informatyka
TIN_K3_K04	Absolwent/ka jest gotów/gotowa do zrozumienia ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia
TIN_K3_K08	Absolwent/ka jest gotów/gotowa do zrozumienia potrzeby popularnego przedstawiania laikom wybranych osiągnięć informatyki
TIN_K3_U01	Absolwent/ka potrafi zastosować wiedzę matematyczną do formułowania, analizowania i rozwiązywania prostych zadań związanych z informatyką oraz do rozwiązywania problemów praktycznych
TIN_K3_U14_inz	Absolwent/ka potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami kompresji i szyfrowania danych
TIN_K3_W01	Absolwent/ka zna i rozumie zagadnienia matematyczne konieczne do zrozumienia podstawowych pojęć i zjawisk niezbędnych w pracy informatyka obejmujące m.in. podstawy analizy matematycznej, przybliżone metody opisu zjawisk ciągłych, metody numeryczne, podstawy algebry i algebry liniowej, podstawy logiki i matematyki dyskretnej, metody probabilistyczne oraz statystykę
TIN_K3_W02_inz	Absolwent/ka zna i rozumie podstawy teorii informacji (entropia, redundancja, kod zwarty), zna procesy przetwarzania informacji
TIN_K3_W03_inz	Absolwent/ka zna i rozumie narzędzia, technologie i urządzenia informatyczne właściwe dla wybranych obszarów zastosowań oraz rozumie podstawy ich działania
TIN_K3_W05_inz	Absolwent/ka zna i rozumie podstawowe metody projektowania, analizowania i programowania algorytmów (projektowanie strukturalne, rekurencja, metoda dziel i zwyciężaj, programowanie z nawrotami, poprawność, metoda niezmienników, złożoność obliczeniowa)
TIN_K3_W06_inz	Absolwent/ka zna i rozumie podstawowe struktury danych i wykonywane na nich operacje (reprezentacja danych liczbowych, arytmetyka i błędy zaokrągleń, tablice, napisy, zbiory, rekordy, pliki, wskaźniki i referencje, struktury wskaźnikowe, listy, stosy, kolejki, drzewa i grafy)
TIN_K3_W10_inz	Absolwent/ka zna i rozumie zagadnienia związane z technologiami sieciowymi, w tym podstawowe protokoły komunikacyjne, bezpieczeństwo i budowa aplikacji sieciowych (siedmiowarstwowy model ISO, protokoły komunikacyjne w tym TCP/IP, trasowanie, model klient-serwer, protokoły kryptograficzne)
TIN_K3_W17	Absolwent/ka zna i rozumie podstawowe zasady bezpieczeństwa i higieny pracy w zawodzie informatyka