KARTA PRZEDMIOTU

Nazwa przedmiotu: ***Kryptografia (TIAu>SI6-Kryp-19)***
Nazwa w języku polskim:
Nazwa w jęz. angielskim: ***Cryptography***

Dane dotyczące przedmiotu:

Jednostka oferująca przedmiot: Wydział Automatyki, Elektroniki i Informatyki
Przedmiot dla jednostki: Politechnika Śląska

Domyślny typ protokołu dla przedmiotu:

ZAL

Język wykładowy:

polski

Strona WWW:

https://platforma2.polsl.pl/rau3/course/view.php?id=297

Skrócony opis:

Celem przedmiotu jest przedstawienie teoretycznych i praktycznych aspektów kryptograficznej ochrony danych. Wykład umożliwia zapoznanie z podstawowymi pojęciami z tego zakresu, zasadami konstrukcji systemów kryptograficznych oraz typami podstawowych prymitywów składowych używanych do ich budowy. Wiedza teoretyczna zdobyta na wykładzie jest stosowana w sposób praktyczny w ramach zajęć projektowych. Zajęcia prowadzone są w formie kontaktowej.

Opis:

Wykład
1. Kryptografia w zarysie. Kryptograficzne funkcje skrótu: a) wymogi, b) popularne algorytmy, c) wybrane zastosowania, d) metody ataku.
2. Szyfry blokowe. Konstrukcja Feistela. Popularne algorytmy. Blokowe tryby działania.
3. Szyfry strumieniowe. Szyfr z kluczem jednorazowym. Generatory klucza; a) wykorzystujące rejestry liniowe, b) wykorzystujące szyfry blokowe. Utajnienie i uwierzytelnienie danych w jednej transakcji.
4. Algorytmy asymetryczne: a) problemy trudne, b) typowe paradygmaty użycia, c) algorytmy tradycyjne: DH, RSA, El-Gamal, DSA, d) algorytmy bazujące na krzywych eliptycznych, e) kanał podprogowy
5. Zarządzanie kluczami: a) SSH, b) PGP, c) SSL/TLS. Uwierzytelnianie użytkowników: wymogi, metody i ataki.
6. Sieć Bitcoin. Inne kryptowaluty.
7. Kryptoanaliza wybranych systemów: a) klonowanie kart SIM z COMP128-1, b) łamanie A5/2, c) łamanie WEP, d) kryptoanaliza HiTag2

Projekt
Szczegółowe zadanie projektowe jest określane osobno dla każdego cyklu. Szczegółowe informacje znajdują się na stronie przedmiotu.
Zadania projektowe obejmują takie zagadnienia jak
1. Opracowanie aplikacji łamiących wybrane systemy,
2. Opracowanie własnych kryptowalut poprzez dostosowanie istniejących,
3. Opracowanie funckji realizujących wybrane operacje kryptograficzne
4. Konfiguracja wybranych narzędzi do ochrony informacji np. serwerów wirtualnych sieci prywatnych,
5. Założenie i prowadzenie wlasnego CA.

Liczba godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów
Wykład: 15h
Projekt: 30h
Zaliczenie wykładu: 2h
Zaliczenie projektu: 4h
Liczba godzin przeznaczonych na pracę własną studenta
Przygotowanie do zaliczenia wykładu: 5h
Przygotowanie projektu: 30h
Przygotowanie prezentacji projektu: 4h
Całkowita liczba godzin: 90
Liczba punktów ECTS: 3
w tym
Liczba punktów ECTS uzyskanych w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów: 1,7

Literatura:

Podstawowa
[1] B. Schneier: Kryptografia dla praktyków, WNT, 1999
Uzupełniająca
[2] N. Ferguson, B. Schneier, T. Kohno: Cryptography Engineering, Wiley, 2010
[3] S. Nakov: Practical Cryptography for Developers, https://cryptobook.nakov.com/

Efekty uczenia się:

Wiedza
Student zna i rozumie
zasady oceny złożoności obliczeniowej algorytmów łamiących zabezpieczenia kryptograficzne, sposoby ochrony informacji we współczesnych systemach teleinformatycznych, zasadę działania systemów kryptowalutowych wykorzystujących blockchain (K1A_W08).

Umiejętności
Student potrafi
przygotować w języku polskim raport dokumentujący zrealizowane inżynierskie zadanie projektowe z zakresu teleinformatyki (K1A_U08), samodzielnie uzupełnić wiedzę niezbędną do zrealizowania zadania projektowego korzystając z dokumentacji sporządzonej w j. angielskim (K1A_U09, K1A_U10)
stworzyć w języku Python prosty system kryptograficzny korzystający
z kryptografii symetrycznej i asymetrycznej (K1A_U28).

Metody i kryteria oceniania:

Wykład
Zaliczenie pisemne w formie testu zawierającego pytania otwarte lub wielokrotnego wyboru
Kryterium zaliczenia: minimum 50% poprawnych odpowiedzi

Projekt
Zaliczenie pisemne w formie pracy projektowej
Kryterium zaliczenia: dostarczenie i zaprezentowanie pracy projektowej

Ocena końcowa: 0.75*Projekt+0.25*Wykład

Sylabus obowiązuje od roku akademickiego 2024/2025, a jego zawartość nie podlega zmianom w trakcie trwania semestru.

Punkty przedmiotu w cyklach:

Teleinformatyka, stacjonarne I stopnia inżynierskie 7 sem. (TIAu-SI7)

Typ punktów	Liczba	Cykl pocz.	Cykl kon.
Europejski System Transferu Punktów (ECTS)	3	2020/2021-Z	