KARTA PRZEDMIOTU

Nazwa przedmiotu: ***Kryptografia danych teleinformatycznych (EiTAu>SM1-23-KDT)***
Nazwa w języku polskim:
Nazwa w jęz. angielskim:

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://platforma.polsl.pl/rau3/course/view.php?id=80236

Skrócony opis:

Celem przedmiotu jest przedstawienie teoretycznych i praktycznych aspektów ochrony danych we współczesnych systemach teleinformatycznych. Wykład umożliwia zapoznanie się z podstawowymi pojęciami z tego zakresu, zasadami konstrukcji systemów kryptograficznych oraz rodzajami prymitywów używanych do ich projektowania. Celem kursu jest przybliżenie praktycznych aspektów ochrony danych.

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

Liczba godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów
Wykład: 15h
Zaliczenie wykładu: 2h
Przygotowanie do zaliczenia wykładu: 8h
Całkowita liczba godzin: 25h
Liczba punktów ECTS: 2

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, K2A_W01

zasady konstrukcji współczesnych systemów kryptograficznych K2A_W09

zasadę działania systemów kryptowalutowych wykorzystujących blockchain. K2A_W08, K2A_W10

Student potrafi:
przygotować w języku Python kod komputerowy realizujący typowe przekształcenie kryptograficzne K2A_U02, K2A_U09, K2A_U11

Student jest gotów do:
oceny zagrożeń wynikających z naruszeń prywatności danych i przeciwdziałania takim zjawiskom K2A_K03, K2A_K04

Metody i kryteria oceniania:

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

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

Punkty przedmiotu w cyklach:

<bez przypisanego programu>

Typ punktów	Liczba	Cykl pocz.	Cykl kon.
Europejski System Transferu Punktów (ECTS)	2	2023/2024-L	