EITC/IS/IST

Teoria bezpieczeństwa informatycznego

Szczegółowa zawartość programowa kursu (15 godz.):

- Definicja informacji (stan klasyczny, źródło wiadomości)
    - Jednostka (bit) i inne jednostki informacji
    - Miara (entropia Shannona)
    - Teoria grafów
    - Prawdopodobieństwo warunkowe
        - Twierdzenie Bayesa
- Ciągi losowe i ciągi pseudolosowe
    - Znaczenie losowości dla bezpieczeństwa
- Wprowadzenie do kodowania
    - Rodzaje kodów
    - Kody Humminga
    - Kompresja
        - Stratna
        - Bezstratna
    - Twierdzenia Shannona
- Kanały komunikacyjne
    - Kanały bezstratne
    - Kanały stratne
        - Rodzaje szumów informacyjnych
    - Procedury korekty błędów
- Podstawowe pojęcia informatyki (algorytm, algebra, język, gramatyka)
- Teoria złożoności obliczeniowej
    - Klasy problemów matematycznych
        - Klasa problemów wielomianowych (P)
        - Klasa problemów wykładniczych (NP)
    - Kontekst kryptografii asymetrycznej
- Modele obliczeniowe
    - Maszyny stanów (Turinga, DAS, NDAS)
        - Twierdzenie Churcha-Turinga
    - Algebra Boole'a i klasyczna teoria układów logicznych
        - Bramki klasyczne
        - Uniwersalność
        - Brak odwracalności binarnej informatyki
        - Realizacje algorytmów
    - Probabilistyczny model obliczeniowy
        - Klasa problemów NBP
        - Rozszerzone twierdzenie Churcha-Turinga
        - Realizacje algorytmów
    - Kwantowy model obliczeniowy
        - Klasa problemów NQP
        - Kwantowa teoria układów logicznych
        - Realizacje algorytmów
        - Fundamentalne zagrożenie kryptografii asymetrycznej
            - Kwantowa transformata Fouriera
            - Algorytm Shora i grupy Kitaeva