EITC/IS/CF

Podstawy kryptografii

Szczegółowa zawartość programowa kursu (15 godz.):

- Poufność
    - Techniki szyfrowania
        - Szyfry przestawieniowe
        - Szyfry podstawieniowe
        - Szyfry macierzowe
        - Klucze
        - XOR
        - OTP
- Wiarygodność
    - Techniki uwierzytelniania
        - Funkcje skrótowe (hashujące)
            - Dyskretny logarytm
            - Ciągi pseudolosowe
            - MD5
    - Integralność
- Kryptologia
    - Kryptografia
    - Kryptoanaliza
    - Steganografia
- Kryptosystemy
    - Asymetryczne (kryptosystemy klucza publicznego)
        - Problemy trudne (klasa problemów NP)
        - Algorytmy asymetryczne
        - Infrastruktura Klucza Publicznego
    - Symetryczne (kryptosystemy klucza prywatnego)
        - Algorytmy symetryczne
        - Dystrybucja klucza prywatnego
        - Kryptografia kwantowa
- Realizacje praktyczne algorytmów
    - Symetryczne
        - Szyfr Vernama
        - DES, IDEA, RC5, 3DES, AES (Rijndael), NASZ
    - Asymetryczne
        - RSA, DH, ElGamal
- Autoryzacja
- Realizacje autoryzacji (hasła, systemy biometryczne)