- 4.1. Wprowadzenie
- 4.2. Sieci podstawieniowo-permutacyjne
- 4.3. Kryptoanaliza liniowa
    - 4.3.1. Lemat nawarstwiania
    - 4.3.2. Liniowe aproksymacje S-boksów
    - 4.3.3. Liniowy atak na SPN
- 4.4. Kryptoanaliza różnicowa
- 4.5. Data Encryption Standard
    - 4.5.1. Opis DES
    - 4.5.2. Analiza DES
- 4.6. Advanced Encryption Standard
    - 4.6.1. Opis AES
    - 4.6.2. Analiza AES
- 4.7. Tryby działania
    - 4.7.1. Atak wyroczni dopełnienia w trybie CBC
- 4.8. Szyfry strumieniowe
    - 4.8.1. Atak korelacyjny na generator kombinacji
    - 4.8.2. Atak algebraiczny na generator filtrów
    - 4.8.3. Trivium
- 4.9. Uwagi i źródła
- Ćwiczenia

- Rozdział 5. Funkcje skrótu i uwierzytelnianie wiadomości

    - 5.1. Funkcje skrótu i integralność danych
    - 5.2. Bezpieczeństwo funkcji skrótu
        - 5.2.1. Model losowej wyroczni
        - 5.2.2. Algorytmy w modelu losowej wyroczni
        - 5.2.3. Porównanie kryteriów bezpieczeństwa
    - 5.3. Iterowane funkcje skrótu
        - 5.3.1. Konstrukcja MerkleaDamgrda
        - 5.3.2. Kilka przykładów iterowanych funkcji skrótów
    - 5.4. Konstrukcja gąbki
        - 5.4.1. SHA-3
    - 5.5. Kody uwierzytelniania wiadomości
        - 5.5.1. Zagnieżdżone kody MAC i HMAC
        - 5.5.2. CBC-MAC
        - 5.5.3. Szyfrowanie uwierzytelnione
    - 5.6. Bezwarunkowo bezpieczne kody MAC
        - 5.6.1. Silnie uniwersalne rodziny skrótów
        - 5.6.2. Optymalność prawdopodobieństwa oszustwa
    - 5.7. Uwagi i źródła
    - Ćwiczenia

- Rozdział 6. Kryptosystem RSA i rozkład liczb całkowitych na czynniki

    - 6.1. Wprowadzenie do kryptografii klucza publicznego
    - 6.2. Więcej teorii liczb
        - 6.2.1. Algorytm Euklidesa
        - 6.2.2. Chińskie twierdzenie o resztach