        - 3.2.1.2.2. Losowy IV
        - 3.2.1.2.3. Jednorazowy IV
      - 3.2.1.3. Dopełnianie
      - 3.2.1.4. Który tryb jest najlepszy?
    - 3.2.2. Szyfry strumieniowe
      - 3.2.2.1. Generowanie ciągów pseudolosowych
        - 3.2.2.1.1. Generatory kongruencyjne
        - 3.2.2.1.2. Generatory oparte na rejestrze przesuwającym ze sprzężeniem zwrotnym
        - 3.2.2.1.3. Generatory oparte na teorii złożoności
      - 3.2.2.2. Generatory ciągów rzeczywiście losowych
      - 3.2.2.3. Najpopularniejsze algorytmy strumieniowe
    - 3.2.3. Szyfr blokowy czy strumieniowy?
  - 3.3. Protokoły kryptograficzne
    - 3.3.1. Protokoły wymiany kluczy
      - 3.3.1.1. Protokół Diffiego-Hellmana
      - 3.3.1.2. KEA
      - 3.3.1.3. Wide-mouth frog
    - 3.3.2. Podpis cyfrowy
      - 3.3.2.1. Niezaprzeczalne podpisy cyfrowe
      - 3.3.2.2. Niepodrabialne podpisy cyfrowe
      - 3.3.2.3. Podpisy ślepe
      - 3.3.2.4. Inne warianty podpisu cyfrowego
    - 3.3.3. Dzielenie sekretów
      - 3.3.3.1. Secret splitting
      - 3.3.3.2. Secret sharing
    - 3.3.4. Inne protokoły
      - 3.3.4.1. Znakowanie czasowe
      - 3.3.4.2. Dowody z wiedzą zerową
      - 3.3.4.3. Kanały podprogowe
      - 3.3.4.4. Protokoły uwierzytelniające
  - 3.4. Infrastruktura klucza publicznego
    - 3.4.1. PKI w teorii
    - 3.4.2. i w praktyce
      - 3.4.2.1. Złożoność
      - 3.4.2.2. Zaufanie
      - 3.4.2.3. Cykl życia klucza
  - 3.5. Kryptografia alternatywna
    - 3.5.1. Fizyka kwantowa w kryptografii
      - 3.5.1.1. Kilka słów o kwantach
      - 3.5.1.2. Kryptografia kwantowa
      - 3.5.1.3. Komputer kwantowy
      - Kryptografia postkwantowa
    - 3.5.2. Kryptografia DNA
      - 3.5.2.1. Struktura DNA
      - 3.5.2.2. Informatyka molekularna
      - 3.5.2.3. Informacja ukryta w DNA
      - 3.5.2.4. Szyfrowanie i deszyfrowanie z wykorzystaniem nukleotydów
    - 3.5.3. Kryptografia wizualna