

- Spis treści
- Wstęp
- Rozdział 1. Wprowadzenie do kryptografii
 - 1.1. Kryptosystemy i podstawowe narzędzia kryptograficzne
 - 1.1.1. Kryptosystemy z kluczem tajnym
 - 1.1.2. Kryptosystemy klucza publicznego
 - 1.1.3. Szyfry blokowe i strumieniowe
 - 1.1.4. Kryptografia hybrydowa
 - 1.2. Integralność wiadomości
 - 1.2.1. Kody uwierzytelniania wiadomości
 - 1.2.2. Schematy podpisów
 - 1.2.3. Niezaprzeczalność
 - 1.2.4. Certyfikaty
 - 1.2.5. Funkcje skrótu
 - 1.3. Protokoły kryptograficzne
 - 1.4. Bezpieczeństwo
 - 1.5. Uwagi i źródła
- Rozdział 2. Klasyczna kryptografia
 - 2.1. Wprowadzenie: niektóre proste kryptosystemy
 - 2.1.1. Szyfr przestawieniowy
 - 2.1.2. Szyfr podstawieniowy
 - 2.1.3. Szyfr afiniczny
 - 2.1.4. Szyfr Vigenrea
 - 2.1.5. Szyfr Hilla
 - 2.1.6. Szyfr permutacyjny
 - 2.1.7. Szyfry strumieniowe
 - 2.2. Kryptoanaliza
 - 2.2.1. Kryptoanaliza szyfru afinicznego
 - 2.2.2. Kryptoanaliza szyfru podstawieniowego
 - 2.2.3. Kryptoanaliza szyfru Vigenrea
 - 2.2.4. Kryptoanaliza szyfru Hilla
 - 2.2.5. Kryptoanaliza szyfru strumieniowego z LFSR
 - 2.3. Uwagi i źródła
 - Ćwiczenia
- Rozdział 3. Teoria Shannona, tajność doskonała i szyfr z kluczem jednorazowym
 - 3.1. Wprowadzenie
 - 3.2. Podstawowa teoria prawdopodobieństwa
 - 3.3. Tajność doskonała
 - 3.4. Entropia
 - 3.4.1. Cechy entropii
 - 3.5. Fałszywe klucze i długość krytyczna
 - 3.6. Uwagi i źródła
 - Ćwiczenia
- Rozdział 4. Szyfry blokowe i szyfry strumieniowe

- 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

- 6.2.3. Inne przydatne fakty
 - 6.3. Kryptosystem RSA
 - 6.3.1. Implementowanie RSA
 - 6.4. Testowanie pierwszości
 - 6.4.1. Symbole Legendrea i Jacobiego
 - 6.4.2. Algorytm SolovayaStrassena
 - 6.4.3. Algorytm MilleraRabina
 - 6.5. Pierwiastki kwadratowe modulo n
 - 6.6. Algorytmy rozkładu na czynniki
 - 6.6.1. Algorytm Pollarda $p-1$
 - 6.6.2. Algorytm rho Pollarda
 - 6.6.3. Algorytm losowych kwadratów Dixona
 - 6.6.4. Algorytmy rozkładu na czynniki w praktyce
 - 6.7. Inne ataki na RSA
 - 6.7.1. Obliczanie (n)
 - 6.7.2. Wykładnik odszyfrowywania
 - 6.7.3. Atak Wienera z małym wykładnikiem odszyfrowywania
 - 6.8. Kryptosystem Rabina
 - 6.8.1. Bezpieczeństwo kryptosystemu Rabina
 - 6.9. Bezpieczeństwo semantyczne RSA
 - 6.9.1. Częściowe informacje dotyczące bitów tekstu jawnego
 - 6.9.2. Uzyskanie bezpieczeństwa semantycznego
 - 6.10. Uwagi i źródła
 - Ćwiczenia
-
- Rozdział 7. Kryptografia klucza publicznego i logarytmy dyskretne
 - 7.1. Wprowadzenie
 - 7.1.1. Kryptosystem ElGamala
 - 7.2. Algorytmy dla problemu logarytmu dyskretnego
 - 7.2.1. Algorytm Shanksa
 - 7.2.2. Algorytm logarytmu dyskretnego rho Pollarda
 - 7.2.3. Algorytm PohligaHellmana
 - 7.2.4. Metoda rachunku indeksowego
 - 7.3. Dolne granice złożoności algorytmów generycznych
 - 7.4. Ciała skończone
 - 7.4.1. Analiza indeksu Joux'a dla ciał o niewielkich wyróżnikach
 - 7.5. Krzywe eliptyczne
 - 7.5.1. Krzywe eliptyczne na liczbach rzeczywistych
 - 7.5.2. Krzywe eliptyczne modulo liczba pierwsza
 - 7.5.3. Krzywe eliptyczne na ciałach skończonych
 - 7.5.4. Własności krzywych eliptycznych
 - 7.5.5. Parowanie krzywych eliptycznych
 - 7.5.6. Kryptosystem ElGamala na krzywych eliptycznych
 - 7.5.7. Obliczanie wielokrotności punktów na krzywych eliptycznych
 - 7.6. Algorytmy logarytmu dyskretnego w praktyce
 - 7.7. Bezpieczeństwo systemów ElGamala
 - 7.7.1. Bitowe bezpieczeństwo logarytmów dyskretnych
 - 7.7.2. Semantyczne bezpieczeństwo systemów ElGamala
 - 7.7.3. Problemy DiffiegoHellmana

- 7.8. Uwagi i źródła
- Ćwiczenia
- Rozdział 8. Schematy podpisów
 - 8.1. Wprowadzenie
 - 8.1.1. Schemat podpisu RSA
 - 8.2. Wymogi bezpieczeństwa dla schematów podpisu
 - 8.2.1. Podpisy i funkcje skrótu
 - 8.3. Schemat podpisu ElGamala
 - 8.3.1. Bezpieczeństwo schematu podpisu ElGamala
 - 8.4. Warianty schematu podpisu ElGamala
 - 8.4.1. Schemat podpisu Schnorra
 - 8.4.2. Algorytm podpisu cyfrowego
 - 8.4.3. DSA krzywej eliptycznej
 - 8.5. Funkcja skrótu o pełnej dziedzinie
 - 8.6. Certyfikaty
 - 8.7. Podpisywanie i szyfrowanie
 - 8.8. Uwagi i źródła
 - Ćwiczenia
- Rozdział 9. Kryptografia postkwantowa
 - 9.1. Wprowadzenie
 - 9.2. Kryptografia oparta na kratkach
 - 9.2.1. NTRU
 - 9.2.2. Kraty i bezpieczeństwo NTRU
 - 9.2.3. LWE
 - 9.3. Kryptografia oparta na kodzie i kryptosystem McEliecea
 - 9.4. Kryptografia wielu zmiennych
 - 9.4.1. Równania ciała ukrytego
 - 9.4.2. Schemat podpisu oliwa i ocet
 - 9.5. Schematy podpisu oparte na skrócie
 - 9.5.1. Schemat podpisu Lamporta
 - 9.5.2. Schemat podpisu Winternitza
 - 9.5.3. Schemat podpisu Merklea
 - 9.6. Uwagi i źródła
 - Ćwiczenia
- Rozdział 10. Schematy identyfikacji i uwierzytelnianie jednostki
 - 10.1. Wprowadzenie
 - 10.1.1. Hasła
 - 10.1.2. Bezpieczne schematy identyfikacji
 - 10.2. Wyzwanie i odpowiedź w kryptografii klucza tajnego
 - 10.2.1. Model ataku i cele przeciwnika
 - 10.2.2. Wzajemne uwierzytelnianie
 - 10.3. Wyzwanie i odpowiedź dla kryptografii klucza publicznego
 - 10.3.1. Schematy identyfikacji klucza publicznego
 - 10.4. Schemat identyfikacji Schnorra

- 10.4.1. Bezpieczeństwo schematu identyfikacji Schnorra
- 10.5. Schemat identyfikacji FeigeaFiataShamira
- 10.6. Uwagi i źródła
- Ćwiczenia
- Rozdział 11. Dystrybucja kluczy
 - 11.1. Wprowadzenie
 - 11.1.1. Modele ataku i cele przeciwników
 - 11.2. Wstępna dystrybucja kluczy
 - 11.2.1. Wstępna dystrybucja kluczy DiffiegoHellmana
 - 11.2.2. Schemat Bloma
 - 11.2.3. Wstępna dystrybucja klucza w sieciach czujnikowych
 - 11.3. Schematy dystrybucji klucza sesji
 - 11.3.1. Schemat NeedhamaSchroedera
 - 11.3.2. Atak DenningaSacca na schemat NS
 - 11.3.3. Kerberos
 - 11.3.4. Schemat BellareaRogawaya
 - 11.4. Ponowne tworzenie klucza i logiczna hierarchia kluczy
 - 11.5. Schematy progowe
 - 11.5.1. Schemat Shamira
 - 11.5.2. Uproszczony schemat (t, t)-progowy
 - 11.5.3. Wizualne schematy progowe
 - 11.6. Uwagi i źródła
 - Ćwiczenia
- Rozdział 12. Schematy uzgadniania klucza
 - 12.1. Wprowadzenie
 - 12.1.1. Bezpieczeństwo warstwy transportu (TLS)
 - 12.2. Uzgodnienie klucza DiffiegoHellmana
 - 12.2.1. Schemat uzgadniania klucza STS (station-to-station)
 - 12.2.2. Bezpieczeństwo STS
 - 12.2.3. Ataki ze znanym kluczem sesji
 - 12.3. Funkcje wyprowadzania klucza
 - 12.4. Schematy MTI uzgadniania klucza
 - 12.4.1. Ataki na MTI/A0 ze znanym kluczem sesji
 - 12.5. Zaprzeczalne schematy uzgadniania klucza
 - 12.6. Aktualizacja kluczy
 - 12.7. Konferencyjne schematy uzgadniania klucza
 - 12.8. Uwagi i źródła
 - Ćwiczenia
- Rozdział 13. Różne tematy
 - 13.1. Kryptografia oparta na tożsamości
 - 13.1.1. Kryptosystem Cocksza oparty na tożsamości
 - 13.1.2. Kryptosystem BonehaFranklina oparty na tożsamości
 - 13.2. Kryptosystem Pailliera
 - 13.3. Ochrona praw autorskich

- 13.3.1. Odciski palca
 - 13.3.2. Identyfikowalna własność nadrzędna
 - 13.3.3. Kody 2-IPP
 - 13.3.4. Śledzenie nielegalnej redystrybucji kluczy
- 13.4. Bitcoin i technologia blockchain
- 13.5. Uwagi i źródła
- Ćwiczenia
- Dodatek A. Teoria liczb i algebraiczne koncepcje kryptografii
 - A.1. Arytmetyka modularna
 - A.2. Grupy
 - A.2.1. Rzędy elementów grupy
 - A.2.2. Grupy cykliczne i elementy pierwotne
 - A.2.3. Podgrupy i warstwy
 - A.2.4. Izomorfizmy i homomorfizmy grup
 - A.2.5. Reszty kwadratowe
 - A.2.6. Algorytm Euklidesa
 - A.2.7. Iloczyny proste
 - A.3. Pierścienie
 - A.3.1. Chińskie twierdzenie o resztach
 - A.3.2. Ideały i pierścienie ilorazowe
 - A.4. Ciała
- Dodatek B. Pseudolosowe generowanie bitów dla kryptografii
 - B.1. Generatory bitów
 - B.2. Bezpieczeństwo pseudolosowych generatorów bitów
 - B.3. Uwagi i źródła
- Bibliografia
- O Autorach
- Przypisy