

- Podziękowania
- Kilka słów wstępu
 - o Jak czytać tę książkę?
- Rozdział 1. Historia kryptografii
 - o 1.1. Prolog Painvin ratuje Francję
 - o 1.2. Początek
 - 1.2.1. Steganografia
 - 1.2.2. Kryptografia
 - 1.2.3. Narodziny kryptoanalizy
 - o 1.3. Rozwój kryptografii i kryptoanalizy
 - 1.3.1. Szyfry homofoniczne
 - 1.3.2. Szyfry polialfabetyczne
 - 1.3.2.1. Tarcza Albertiego
 - 1.3.2.2. Tabula recta
 - 1.3.2.3. Le chiffre indechiffable
 - 1.3.2.4. Złamanie szyfru nie do złamania
 - 1.3.3. Szyfry digraficzne
 - 1.3.4. Prawdziwy szyfr nie do złamania
 - 1.3.5. Kamienie milowe kryptografii
 - o 1.4. Kryptografia II wojny światowej
 - 1.4.1. Enigma i Colossus
 - 1.4.1.1. Jak działała Enigma?
 - 1.4.1.2. Cyklometr i Bomby
 - 1.4.1.3. Bletchley Park
 - 1.4.1.4. Colossus
 - o 1.5. Era komputerów
 - 1.5.1. DES
 - 1.5.2. Narodziny kryptografii asymetrycznej
 - 1.5.3. RSA
 - 1.5.4. PGP
 - 1.5.5. Ujawniona tajemnica
 - 1.5.6. Upowszechnienie kryptografii
- Rozdział 2. Matematyczne podstawy kryptografii
 - o 2.1. Podstawowe pojęcia
 - 2.1.1. Słownik tekstu jawnego
 - 2.1.2. Przestrzeń tekstu
 - 2.1.3. Iloczyn kartezjański
 - 2.1.4. System kryptograficzny
 - 2.1.5. Szyfrowanie monoalfabetyczne
 - 2.1.6. Funkcje jednokierunkowe
 - 2.1.7. Arytmetyka modulo
 - 2.1.8. Dwójkowy system liczbowy
 - 2.1.9. Liczby pierwsze
 - 2.1.9.1. Co to za liczby i ile ich jest?
 - 2.1.9.2. Sito Eratostenesa
 - 2.1.9.3. Sito Sundarama
 - 2.1.9.4. Sito Atkina
 - 2.1.9.5. Liczby pierwsze Mersennea i nie tylko
 - 2.1.9.6. Małe twierdzenie Fermata
 - 2.1.9.7. NWD i NWW

- 2.1.10. Logarytmy
 - 2.1.11. Grupy, pierścienie i ciała
 - 2.1.11.1. Grupa
 - 2.1.11.2. Pierścień
 - 2.1.11.3. Ciało
 - 2.1.12. Izomorfizmy
 - 2.1.12.1. Funkcja różnowartościowa
 - 2.1.12.2. Surjekcja
 - 2.1.12.3. Przekształcenie izomorficzne
- o 2.2. Wzory w praktyce
 - 2.2.1. Kryptosystem RSA
 - 2.2.2. Problem faktoryzacji dużych liczb
 - 2.2.3. Mocne liczby pierwsze
 - 2.2.4. Generowanie liczb pierwszych
 - 2.2.4.1. Test Lehmana
 - 2.2.4.2. Test Rabina-Millera
 - 2.2.4.3. Test Solovaya-Strassena
 - 2.2.4.4. Test Fermata
 - 2.2.5. Chińskie twierdzenie o resztach
 - 2.2.6. Logarytm dyskretny
 - 2.2.7. XOR i AND
 - 2.2.8. Testy zgodności
 - 2.2.8.1. Zdarzenia i ich prawdopodobieństwo
 - 2.2.8.2. Test zgodności Kappa
 - 2.2.8.3. Test zgodności Fi
 - 2.2.9. Złożoność algorytmów
 - 2.2.10. Teoria informacji
 - 2.2.10.1. Entropia
 - 2.2.10.2. Nadmiarowość i zawartość informacyjna języka
 - 2.2.10.3. Odległość jednostkowa
 - 2.2.10.4. Jak to wygląda w praktyce?
 - 2.2.10.5. Mieszanie i rozpraszanie
- Rozdział 3. Kryptografia w teorii
 - o 3.1. Ataki kryptoanalityczne i nie tylko
 - 3.1.1. Metody kryptoanalityczne
 - 3.1.2. Kryptoanaliza liniowa i różnicowa
 - 3.1.2.1. Kryptoanaliza różnicowa
 - 3.1.2.2. Kryptoanaliza liniowa
 - 3.1.3. Inne rodzaje ataków
 - o 3.2. Rodzaje i tryby szyfrowania
 - 3.2.1. Szyfry blokowe
 - 3.2.1.1. Tryby szyfrów blokowych
 - 3.2.1.1.1. ECB
 - 3.2.1.1.2. CBC
 - 3.2.1.1.3. CFB
 - 3.2.1.1.4. OFB
 - 3.2.1.1.5. CTR
 - 3.2.1.1.6. Inne tryby szyfrowania blokowego
 - 3.2.1.2. Kilka słów o wektorach inicjujących
 - 3.2.1.2.1. IV jako licznik

- 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?
- o 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
- o 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
- o 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

- 3.5.3.1. Udziały
 - 3.5.3.2. Schemat progowy
 - o 3.6. Współczesna steganografia
 - 3.6.1. Znaki wodne
 - 3.6.1.1. Algorytm LSB
 - 3.6.1.2. Algorytm Patchwork
 - 3.6.2. Oprogramowanie steganograficzne
- Rozdział 4. Kryptografia w praktyce
 - o 4.1. Konstrukcja bezpiecznego systemu kryptograficznego
 - 4.1.1. Wybór i implementacja kryptosystemu
 - 4.1.2. Bezpieczny system kryptograficzny
 - 4.1.3. Najśłabsze ogniwo
 - 4.1.3.1. Kryptografia jako gwarancja bezpieczeństwa
 - 4.1.3.2. Hasła
 - 4.1.3.3. Procedury kontra socjotechnika
 - 4.1.3.4. Wewnętrzny wróg
 - 4.1.3.5. Podsumowując
 - o 4.2. Zabezpieczanie połączeń internetowych
 - 4.2.1. Protokół TLS
 - 4.2.1.1. Struktura i lokalizacja protokołu TLS
 - 4.2.1.2. Nawiązywanie połączenia w TLS
 - 4.2.1.3. Wyznaczanie kluczy
 - 4.2.1.4. Przesyłanie danych
 - 4.2.1.5. Implementacja protokołu TLS
 - 4.2.1.6. Sprawdzanie certyfikatu
 - 4.2.1.7. Biblioteka OpenSSL
 - 4.2.2. Protokół SSH
 - 4.2.2.1. Sesja SSH
 - 4.2.2.1.1. Uwierzytelnianie serwera
 - 4.2.2.1.2. Ustanawianie bezpiecznego połączenia
 - 4.2.2.1.3. Uwierzytelnianie klienta
 - 4.2.2.2. Algorytmy wykorzystywane w SSH
 - 4.2.2.3. SSH1 a SSH2
 - 4.2.2.4. PuTTY
 - o 4.3. Symantec Encryption Desktop
 - 4.3.1. PGP Keys
 - 4.3.2. PGP Messaging
 - 4.3.3. PGP Zip
 - 4.3.4. PGP Disk
 - 4.3.4.1. Tworzenie dysków wirtualnych
 - 4.3.4.2. Szyfrowanie całego dysku lub partycji
 - 4.3.4.3. Czyszczenie wolnej przestrzeni dyskowej
 - 4.3.5. PGP Viewer
 - 4.3.6. File Share Encryption
 - 4.3.7. PGP Shredder
 - 4.3.8. Web of Trust
 - o 4.4. GnuPG
 - 4.4.1. Tworzenie certyfikatu
 - 4.4.1.1. Tworzenie certyfikatu X.509
 - 4.4.1.2. Tworzenie certyfikatu OpenPGP

- 4.4.2. Obsługa certyfikatów
 - 4.4.3. Szyfrowanie i podpisywanie
 - 4.4.4. Obsługa serwerów
- o 4.5. TrueCrypt
 - 4.5.1. Tworzenie szyfrowanych dysków i partycji
 - 4.5.2. Obsługa dysków wirtualnych
 - 4.5.3. Ukryte dyski
 - 4.5.4. Pozostałe opcje i polecenia
- o 4.6. Składanie i weryfikacja podpisów elektronicznych
 - 4.6.1. Wymagania techniczne
 - 4.6.1.1. Obsługa certyfikatów
 - 4.6.1.2. Obsługa 128-bitowej siły szyfrowania
 - 4.6.1.3. Obsługa cookies
 - 4.6.1.4. Obsługa ActiveX
 - 4.6.2. Jak zdobyć certyfikat cyfrowy?
 - 4.6.2.1. Centra certyfikacji
 - 4.6.2.2. Uzyskiwanie certyfikatu
 - 4.6.3. O czym warto pamiętać?
 - 4.6.4. Konfiguracja programu pocztowego
 - 4.6.4.1. Microsoft Outlook
 - 4.6.4.2. MS Outlook Express
 - 4.6.4.3. Mozilla Thunderbird
 - 4.6.4.4. Informacje dodatkowe
 - 4.6.5. Struktura certyfikatu
 - 4.6.5.1. Elementy certyfikatu
 - 4.6.5.2. Uzyskiwanie informacji o certyfikacie
- o 4.7. Kryptografia w PHP i MySQL
 - 4.7.1. Funkcje szyfrujące w PHP
 - 4.7.1.1. Biblioteka mcrypt
 - 4.7.1.2. Dostępne algorytmy
 - 4.7.1.3. Wywoływanie funkcji szyfrujących
 - 4.7.1.4. Kilka pożytecznych uwag
 - 4.7.2. Szyfrowanie danych w MySQL
 - 4.7.2.1. Przykładowe funkcje
 - 4.7.2.2. Szyfrowanie danych
 - 4.7.3. Kolejne udoskonalenia
- Podsumowanie
- Dodatek A. Jednokierunkowe funkcje skrótu
 - o A.1. MD5
 - A.1.1. Przekształcenia początkowe
 - A.1.2. Pętla główna MD5
 - A.1.3. Obliczenia końcowe
 - o A.2. SHA-1
 - A.2.1. Przekształcenia początkowe
 - A.2.2. Pętla główna algorytmu SHA-1
 - A.2.3. Operacje w cyklu SHA-1
 - A.2.4. Obliczenia końcowe
 - o A.3. SHA-2
 - A.3.1. Dodatkowe pojęcia
 - A.3.2. Przekształcenia początkowe

- A.3.3. Operacje w cyklu SHA-2
 - A.3.4. Dodatkowe różnice między algorytmami SHA-2
 - o A.4. SHA-3
 - A.4.1. SHA-3 ogólny opis
 - A.4.2. Funkcja rundy SHA-3
 - A.4.3. Funkcja mieszająca SHA-3
 - o A.5. Inne funkcje skrótu
- Dodatek B. Algorytmy szyfrujące
 - o B.1. IDEA
 - B.1.1. Przekształcenia początkowe
 - B.1.2. Operacje pojedynczego cyklu IDEA
 - B.1.3. Generowanie podkluczy
 - B.1.4. Przekształcenia MA
 - B.1.5. Deszyfrowanie IDEA
 - o B.2. DES
 - B.2.1. Permutacja początkowa (IP)
 - B.2.2. Podział tekstu na bloki
 - B.2.3. Permutacja rozszerzona
 - B.2.4. S-bloki
 - B.2.5. P-bloki
 - B.2.6. Permutacja końcowa
 - B.2.7. Deszyfrowanie DES
 - B.2.8. Modyfikacje DES
 - B.2.8.1. 2DES
 - B.2.8.2. 3DES
 - B.2.8.3. DES z S-blokami zależnymi od klucza
 - B.2.8.4. DESX
 - o B.3. AES
 - B.3.1. Opis algorytmu
 - B.3.2. Generowanie kluczy
 - B.3.2.1. Rozszerzanie klucza
 - B.3.2.2. Selekcja podkluczy
 - B.3.3. Pojedyncza runda algorytmu
 - B.3.3.1. ByteSub
 - B.3.3.2. ShiftRow
 - B.3.3.3. MixColumn
 - B.3.3.4. AddRoundKey
 - B.3.4. Podsumowanie
 - o B.4. Twofish
 - B.4.1. Opis algorytmu
 - B.4.2. Pojedyncza runda algorytmu
 - B.4.2.1. Funkcja g
 - B.4.2.2. Przekształcenie PHT
 - B.4.2.3. Dodanie kluczy szyfrowania
 - B.4.3. Podsumowanie
 - o B.5. CAST5
 - B.5.1. Opis algorytmu
 - B.5.2. Rundy CAST5
 - o B.6. Blowfish
 - B.6.1. Opis algorytmu

- B.6.2. Funkcja algorytmu Blowfish
- o B.7. DSA
 - B.7.1. Podpisywanie wiadomości
 - B.7.2. Weryfikacja podpisu
 - B.7.3. Inne warianty DSA
 - B.7.3.1. Wariant pierwszy
 - B.7.3.2. Wariant drugi
- o B.8. RSA
 - B.8.1. Generowanie pary kluczy
 - B.8.2. Szyfrowanie i deszyfrowanie
- o B.9. Inne algorytmy szyfrujące
- Dodatek C. Kryptografia w służbie historii
 - o C.1. Święte rysunki
 - C.1.1. 1000 lat później
 - C.1.2. Szyfr faraonów
 - C.1.3. Ziarno przeznaczenia
 - C.1.4. Je tiens laffaire!
 - C.1.5. Tajemnica hieroglifów
 - o C.2. Język mitów
 - C.2.1. Mit, który okazał się prawdziwy
 - C.2.2. Trojaczki Kober
 - C.2.3. Raport z półwiecza
 - o C.3. Inne języki
- Bibliografia