

## **Kilka słów wstępu (9)**

### **Rozdział 1. Historia kryptografii (11)**

- 1.1. Prolog - Painvin ratuje Francję (11)
- 1.2. Początek... (15)
  - 1.2.1. Steganografia (15)
  - 1.2.2. Kryptografia (16)
  - 1.2.3. Narodziny kryptoanalizy (17)
- 1.3. Rozwój kryptografii i kryptoanalizy (19)
  - 1.3.1. Szyfry homofoniczne (19)
  - 1.3.2. Szyfry polialfabetyczne (20)
  - 1.3.3. Szyfry digraficzne (25)
  - 1.3.4. Kamienie milowe kryptografii (27)
- 1.4. Kryptografia II wojny światowej (28)
  - 1.4.1. Enigma i Colossus (28)
- 1.5. Era komputerów (33)
  - 1.5.1. DES (34)
  - 1.5.2. Narodziny kryptografii asymetrycznej (35)
  - 1.5.3. RSA (36)
  - 1.5.4. PGP (37)
  - 1.5.5. Ujawniona tajemnica (38)
  - 1.5.6. Upowszechnienie kryptografii (39)

### **Rozdział 2. Matematyczne podstawy kryptografii (41)**

- 2.1. Podstawowe pojęcia (41)
  - 2.1.1. Słownik tekstu jawnego (42)
  - 2.1.2. Przestrzeń tekstu (42)
  - 2.1.3. Iloczyn kartezjański (42)
  - 2.1.4. System kryptograficzny (44)
  - 2.1.5. Szyfrowanie monoalfabetyczne (45)
  - 2.1.6. Funkcje jednokierunkowe (45)
  - 2.1.7. Arytmetyka modulo (46)
  - 2.1.8. Dwójkowy system liczbowy (47)
  - 2.1.9. Liczby pierwsze (48)
  - 2.1.10. Logarytmy (52)
  - 2.1.11. Grupy, pierścienie i ciała (52)
  - 2.1.12. Izomorfizmy (54)
- 2.2. Wzory w praktyce (55)
  - 2.2.1. Kryptosystem RSA (56)
  - 2.2.2. Problem faktoryzacji dużych liczb (57)
  - 2.2.3. Mocne liczby pierwsze (59)
  - 2.2.4. Generowanie liczb pierwszych (59)
  - 2.2.5. Chińskie twierdzenie o resztach (61)
  - 2.2.6. Logarytm dyskretny (62)
  - 2.2.7. XOR i AND (63)
  - 2.2.8. Testy zgodności (64)
  - 2.2.9. Złożoność algorytmów (73)
  - 2.2.10. Teoria informacji (74)

## **Rozdział 3. Kryptografia w teorii (79)**

- 3.1. Ataki kryptoanalityczne i nie tylko (79)
  - 3.1.1. Metody kryptoanalityczne (79)
  - 3.1.2. Kryptoanaliza liniowa i różnicowa (81)
  - 3.1.3. Inne rodzaje ataków (82)
- 3.2. Rodzaje i tryby szyfrowania (87)
  - 3.2.1. Szyfry blokowe (87)
  - 3.2.2. Szyfry strumieniowe (96)
  - 3.2.3. Szyfr blokowy czy strumieniowy? (101)
- 3.3. Protokoły kryptograficzne (102)
  - 3.3.1. Protokoły wymiany kluczy (102)
  - 3.3.2. Podpis cyfrowy (106)
  - 3.3.3. Dzielenie sekretów (109)
  - 3.3.4. Inne protokoły (111)
- 3.4. Infrastruktura klucza publicznego (115)
  - 3.4.1. PKI w teorii... (115)
  - 3.4.2. ...i w praktyce (115)
- 3.5. Kryptografia alternatywna (118)
  - 3.5.1. Fizyka kwantowa w kryptografii (118)
  - 3.5.2. Kryptografia DNA (123)
  - 3.5.3. Kryptografia wizualna (127)

## **Rozdział 4. Kryptografia w praktyce (131)**

- 4.1. Konstrukcja bezpiecznego systemu kryptograficznego (131)
  - 4.1.1. Wybór i implementacja kryptosystemu (132)
  - 4.1.2. Bezpieczny system kryptograficzny (133)
  - 4.1.3. Najślabsze ogniwo (134)
- 4.2. Zabezpieczanie połączeń internetowych (137)
  - 4.2.1. Protokół SSL (138)
  - 4.2.2. Protokół SSH (146)
- 4.3. Pakiet PGP (153)
  - 4.3.1. PGPkeys (153)
  - 4.3.2. PGPmail (156)
  - 4.3.3. PGPdisk (164)
  - 4.3.4. Standard PGP/MIME (171)
  - 4.3.5. Web of Trust (172)
- 4.4. Składanie i weryfikacja podpisów elektronicznych (175)
  - 4.4.1. Wymagania techniczne (175)
  - 4.4.2. Jak zdobyć certyfikat cyfrowy? (177)
  - 4.4.3. O czym warto pamiętać? (180)
  - 4.4.4. Konfiguracja programu pocztowego (181)
  - 4.4.5. Struktura certyfikatu (186)
- 4.5. Kryptografia w PHP i MySQL (188)
  - 4.5.1. Funkcje szyfrujące w PHP (189)
  - 4.5.2. Szyfrowanie danych w MySQL (194)

## **Podsumowanie (197)**

## **Dodatek A Jednokierunkowe funkcje skrótów (199)**

- A.1. SHA (199)
  - A.1.1. Przekształcenia początkowe (199)
  - A.1.2. Pętla główna algorytmu SHA (200)
  - A.1.3. Operacje w cyklu SHA (200)
  - A.1.4. Obliczenia końcowe (201)
- A.2. MD5 (202)
  - A.2.1. Przekształcenia początkowe (202)
  - A.2.2. Pętla główna MD5 (202)
  - A.2.3. Obliczenia końcowe (204)

## **Dodatek B Algorytmy szyfrujące (207)**

- B.1. IDEA (207)
  - B.1.1. Przekształcenia początkowe (207)
  - B.1.2. Operacje pojedynczego cyklu IDEA (207)
  - B.1.3. Generowanie podkluczy (209)
  - B.1.4. Przekształcenia MA (skrót od ang. multiplication-addition) (209)
  - B.1.5. Deszyfrowanie IDEA (209)
- B.2. DES (211)
  - B.2.1. Permutacja początkowa (IP) (211)
  - B.2.2. Podział tekstu na bloki (211)
  - B.2.3. Permutacja rozszerzona (214)
  - B.2.4. S-bloki (ang. S-boxes) (214)
  - B.2.5. P-bloki (216)
  - B.2.6. Permutacja końcowa (216)
  - B.2.7. Deszyfrowanie DES (216)
  - B.2.8. Modyfikacje DES (217)
- B.3. AES (219)
  - B.3.1. Opis algorytmu (219)
  - B.3.2. Generowanie kluczy (220)
  - B.3.3. Pojedyncza runda algorytmu (221)
  - B.3.4. Podsumowanie (223)
- B.4. Twofish (223)
  - B.4.1. Opis algorytmu (223)
  - B.4.2. Pojedyncza runda algorytmu (225)
  - B.4.3. Podsumowanie (229)
- B.5. CAST5 (229)
  - B.5.1. Opis algorytmu (229)
  - B.5.2. Rundy CAST5 (229)
- B.6. DSA (231)
  - B.6.1. Podpisywanie wiadomości (231)
  - B.6.2. Weryfikacja podpisu (232)
  - B.6.3. Inne warianty DSA (232)
- B.7. RSA (233)
  - B.7.1. Generowanie pary kluczy (234)
  - B.7.2. Szyfrowanie i deszyfrowanie (234)
- B.8. Inne algorytmy szyfrujące (234)

## **Dodatek C Kryptografia w służbie historii (237)**

- C.1. Święte rysunki (238)
  - C.1.1. 1000 lat później... (239)
  - C.1.2. Szyfr faraonów (240)
  - C.1.3. Ziarno przeznaczenia (242)
  - C.1.4. Je tiens l'affaire! (243)
  - C.1.5. Tajemnica hieroglifów (243)
- C.2. Język mitów (244)
  - C.2.1. Mit, który okazał się prawdziwy (244)
  - C.2.2. Trojaczki Kober (247)
  - C.2.3. Raport z półwecza (248)
- C.3. Inne języki (252)

**Bibliografia (253)**

**Skorowidz (255)**