

Spis treści

Kilka słów wstępu	9
Rozdział 1. Historia kryptografii	13
1.1. Prolog — Painvin ratuje Francję	13
1.2. Początek... ..	17
1.2.1. Steganografia	17
1.2.2. Kryptografia	18
1.2.3. Narodziny kryptoanalizy	20
1.3. Rozwój kryptografii i kryptoanalizy	21
1.3.1. Szyfry homofoniczne	21
1.3.2. Szyfry polialfabetyczne	22
1.3.3. Szyfry digraficzne	27
1.3.4. Kamienie milowe kryptografii	28
1.4. Kryptografia II wojny światowej	29
1.4.1. Enigma i Colossus	30
1.5. Era komputerów	35
1.5.1. DES	36
1.5.2. Narodziny kryptografii asymetrycznej	37
1.5.3. RSA	37
1.5.4. PGP	38
1.5.5. Ujawniona tajemnica	40
1.5.6. Upowszechnienie kryptografii	40
Rozdział 2. Matematyczne podstawy kryptografii	43
2.1. Podstawowe pojęcia	44
2.1.1. Słownik tekstu jawnego	44
2.1.2. Przestrzeń tekstu	44
2.1.3. Iloczyn kartezjański	45
2.1.4. System kryptograficzny	46
2.1.5. Szyfrowanie monoalfabetyczne	47
2.1.6. Funkcje jednokierunkowe	47
2.1.7. Arytmetyka modulo	48
2.1.8. Dwójkowy system liczbowy	49
2.1.9. Liczby pierwsze	50
2.1.10. Logarytmy	54
2.1.11. Grupy, pierścienie i ciała	54
2.1.12. Izomorfizmy	56

2.2. Wzory w praktyce	57
2.2.1. Kryptosystem RSA	58
2.2.2. Problem faktoryzacji dużych liczb	60
2.2.3. Mocne liczby pierwsze	61
2.2.4. Generowanie liczb pierwszych	62
2.2.5. Chińskie twierdzenie o resztach	64
2.2.6. Logarytm dyskretny	65
2.2.7. XOR i AND	66
2.2.8. Testy zgodności	67
2.2.9. Złożoność algorytmów	76
2.2.10. Teoria informacji	77

Rozdział 3. Kryptografia w teorii 83

3.1. Ataki kryptoanalityczne i nie tylko	83
3.1.1. Metody kryptoanalityczne	83
3.1.2. Kryptoanaliza liniowa i różnicowa	85
3.1.3. Inne rodzaje ataków	87
3.2. Rodzaje i tryby szyfrowania	92
3.2.1. Szyfry blokowe	92
3.2.2. Szyfry strumieniowe	101
3.2.3. Szyfr blokowy czy strumieniowy?	106
3.3. Protokoły kryptograficzne	107
3.3.1. Protokoły wymiany kluczy	107
3.3.2. Podpis cyfrowy	111
3.3.3. Dzielenie sekretów	114
3.3.4. Inne protokoły	116
3.4. Infrastruktura klucza publicznego	120
3.4.1. PKI w teorii... ..	121
3.4.2. ...i w praktyce	121
3.5. Kryptografia alternatywna	124
3.5.1. Fizyka kwantowa w kryptografii	124
3.5.2. Kryptografia DNA	130
3.5.3. Kryptografia wizualna	134
3.6. Współczesna steganografia	136
3.6.1. Znaki wodne	136
3.6.2. Oprogramowanie steganograficzne	138

Rozdział 4. Kryptografia w praktyce 141

4.1. Konstrukcja bezpiecznego systemu kryptograficznego	141
4.1.1. Wybór i implementacja kryptosystemu	142
4.1.2. Bezpieczny system kryptograficzny	143
4.1.3. Najslabsze ogniwo	144
4.2. Zabezpieczanie połączeń internetowych	148
4.2.1. Protokół SSL	148
4.2.2. Protokół SSH	156
4.3. PGP	164
4.3.1. PGPkeys	164
4.3.2. PGPmail	167
4.3.3. PGPdisk	175
4.3.4. Standard PGP/MIME	182
4.3.5. Web of Trust	183
4.3.6. PGP 9.x	186

4.4. GnuPG	188
4.4.1. Generowanie klucza prywatnego	188
4.4.2. Obsługa programu	189
4.5. TrueCrypt	196
4.5.1. Tworzenie szyfrowanych dysków i partycji	197
4.5.2. Obsługa dysków wirtualnych	199
4.5.3. Ukryte dyski	200
4.5.4. Pozostałe opcje i polecenia	202
4.6. Składanie i weryfikacja podpisów elektronicznych	204
4.6.1. Wymagania techniczne	204
4.6.2. Jak zdobyć certyfikat cyfrowy?	206
4.6.3. O czym warto pamiętać?	209
4.6.4. Konfiguracja programu pocztowego	209
4.6.5. Struktura certyfikatu	215
4.7. Kryptografia w PHP i MySQL	217
4.7.1. Funkcje szyfrujące w PHP	217
4.7.2. Szyfrowanie danych w MySQL	222
4.7.3. Kolejne udoskonalenia	224
Podsumowanie	227
Dodatek A Jednokierunkowe funkcje skrótu	229
A.1. MD5	229
A.1.1. Przekształcenia początkowe	229
A.1.2. Pętla główna MD5	230
A.1.3. Obliczenia końcowe	232
A.2. SHA-1	232
A.2.1. Przekształcenia początkowe	232
A.2.2. Pętla główna algorytmu SHA-1	233
A.2.3. Operacje w cyklu SHA-1	233
A.2.4. Obliczenia końcowe	234
A.3. SHA-2	235
A.3.1. Dodatkowe pojęcia	235
A.3.2. Przekształcenia początkowe	236
A.3.3. Operacje w cyklu SHA-2	237
A.3.4. Dodatkowe różnice między algorytmami SHA-2	239
Inne funkcje skrótu	240
Dodatek B Algorytmy szyfrujące	241
B.1. IDEA	241
B.1.1. Przekształcenia początkowe	241
B.1.2. Operacje pojedynczego cyklu IDEA	241
B.1.3. Generowanie podkluczy	243
B.1.4. Przekształcenia MA	243
B.1.5. Deszyfrowanie IDEA	243
B.2. DES	245
B.2.1. Permutacja początkowa (IP)	245
B.2.2. Podział tekstu na bloki	245
B.2.3. Permutacja rozszerzona	247
B.2.4. S-bloki	248
B.2.5. P-bloki	249
B.2.6. Permutacja końcowa	250
B.2.7. Deszyfrowanie DES	250
B.2.8. Modyfikacje DES	251

B.3. AES	253
B.3.1. Opis algorytmu	253
B.3.2. Generowanie kluczy	253
B.3.3. Pojedyncza runda algorytmu	254
B.3.4. Podsumowanie	256
B.4. Twofish	256
B.4.1. Opis algorytmu	257
B.4.2. Pojedyncza runda algorytmu	257
B.4.3. Podsumowanie	261
B.5. CAST5	262
B.5.1. Opis algorytmu	262
B.5.2. Rundy CAST5	263
B.6. DSA	263
B.6.1. Podpisywanie wiadomości	264
B.6.2. Weryfikacja podpisu	264
B.6.3. Inne warianty DSA	265
B.7. RSA	266
B.7.1. Generowanie pary kluczy	266
B.7.2. Szyfrowanie i deszyfrowanie	266
B.8. Inne algorytmy szyfrujące	267
Dodatek C Kryptografia w służbie historii	269
C.1. Święte rysunki	270
C.1.1. 1000 lat później...	271
C.1.2. Szyfr faraonów	272
C.1.3. Ziarno przeznaczenia	273
C.1.4. Je tiens l'affaire!	274
C.1.5. Tajemnica hieroglifów	275
C.2. Język mitów	276
C.2.1. Mit, który okazał się prawdziwy	276
C.2.2. Trojaczki Kober	279
C.2.3. Raport z półwiecza	280
C.3. Inne języki	283
Bibliografia	285
Skorowidz	287