

Spis treści

Kilka słów wstępu	11
-------------------------	----

Rozdział 1. Historia kryptografii	15
--	-----------

1.1. Prolog — Painvin ratuje Francję	15
1.2. Początek	19
1.2.1. Steganografia	19
1.2.2. Kryptografia	20
1.2.3. Narodziny kryptoanalizy	22
1.3. Rozwój kryptografii i kryptoanalizy	23
1.3.1. Szyfry homofoniczne	23
1.3.2. Szyfry polialfabetyczne	24
1.3.3. Szyfry digraficzne	29
1.3.4. Prawdziwy „szyfr nie do złamania”	30
1.3.5. Kamienie milowe kryptografii	32
1.4. Kryptografia II wojny światowej	33
1.4.1. Enigma i Colossus	33
1.5. Era komputerów	38
1.5.1. DES	39
1.5.2. Narodziny kryptografii asymetrycznej	40
1.5.3. RSA	41
1.5.4. PGP	42
1.5.5. Ujawniona tajemnica	43
1.5.6. Upowszechnienie kryptografii	44

Rozdział 2. Matematyczne podstawy kryptografii	47
---	-----------

2.1. Podstawowe pojęcia	48
2.1.1. Słownik tekstu jawnego	48
2.1.2. Przestrzeń tekstu	48
2.1.3. Iloczyn kartezjański	49
2.1.4. System kryptograficzny	50
2.1.5. Szyfrowanie monoalfabetyczne	51
2.1.6. Funkcje jednokierunkowe	51
2.1.7. Arytmetyka modulo	52
2.1.8. Dwójkowy system liczbowy	53
2.1.9. Liczby pierwsze	54
2.1.10. Logarytmy	59
2.1.11. Grupy, pierścienie i ciała	60
2.1.12. Izomorfizmy	61

2.2. Wzory w praktyce	63
2.2.1. Kryptosystem RSA	63
2.2.2. Problem faktoryzacji dużych liczb	65
2.2.3. Mocne liczby pierwsze	67
2.2.4. Generowanie liczb pierwszych	67
2.2.5. Chińskie twierdzenie o resztach	70
2.2.6. Logarytm dyskretny	70
2.2.7. XOR i AND	72
2.2.8. Testy zgodności	73
2.2.9. Złożoność algorytmów	82
2.2.10. Teoria informacji	83

Rozdział 3. Kryptografia w teorii 89

3.1. Ataki kryptoanalityczne i nie tylko	89
3.1.1. Metody kryptoanalityczne	89
3.1.2. Kryptoanaliza liniowa i różnicowa	91
3.1.3. Inne rodzaje ataków	92
3.2. Rodzaje i tryby szyfrowania	98
3.2.1. Szyfry blokowe	98
3.2.2. Szyfry strumieniowe	107
3.2.3. Szyfr blokowy czy strumieniowy?	112
3.3. Protokoły kryptograficzne	113
3.3.1. Protokoły wymiany kluczy	113
3.3.2. Podpis cyfrowy	117
3.3.3. Dzielenie sekretów	120
3.3.4. Inne protokoły	123
3.4. Infrastruktura klucza publicznego	126
3.4.1. PKI w teorii... ..	127
3.4.2. ...i w praktyce	127
3.5. Kryptografia alternatywna	130
3.5.1. Fizyka kwantowa w kryptografii	130
3.5.2. Kryptografia DNA	137
3.5.3. Kryptografia wizualna	142
3.6. Współczesna steganografia	144
3.6.1. Znaki wodne	144
3.6.2. Oprogramowanie steganograficzne	145

Rozdział 4. Kryptografia w praktyce 147

4.1. Konstrukcja bezpiecznego systemu kryptograficznego	147
4.1.1. Wybór i implementacja kryptosystemu	148
4.1.2. Bezpieczny system kryptograficzny	149
4.1.3. Najsłabsze ogniwo	150
4.2. Zabezpieczanie połączeń internetowych	154
4.2.1. Protokół TLS	154
4.2.2. Protokół SSH	162
4.3. Symantec Encryption Desktop	169
4.3.1. PGP Keys	173
4.3.2. PGP Messaging	177
4.3.3. PGP Zip	181
4.3.4. PGP Disk	185
4.3.5. PGP Viewer	194
4.3.6. File Share Encryption	196
4.3.7. PGP Shredder	198
4.3.8. Web of Trust	199

4.4. GnuPG	201
4.4.1. Tworzenie certyfikatu	201
4.4.2. Obsługa certyfikatów	203
4.4.3. Szyfrowanie i podpisywanie	205
4.4.4. Obsługa serwerów	209
4.5. TrueCrypt	210
4.5.1. Tworzenie szyfrowanych dysków i partycji	210
4.5.2. Obsługa dysków wirtualnych	213
4.5.3. Ukryte dyski	213
4.5.4. Pozostałe opcje i polecenia	215
4.6. Składanie i weryfikacja podpisów elektronicznych	218
4.6.1. Wymagania techniczne	218
4.6.2. Jak zdobyć certyfikat cyfrowy?	219
4.6.3. O czym warto pamiętać?	221
4.6.4. Konfiguracja programu pocztowego	222
4.6.5. Struktura certyfikatu	226
4.7. Kryptografia w PHP i MySQL	229
4.7.1. Funkcje szyfrujące w PHP	229
4.7.2. Szyfrowanie danych w MySQL	234
4.7.3. Kolejne udoskonalenia	238

Podsumowanie 241

Dodatek A Jednokierunkowe funkcje skrótu 243

A.1. MD5	243
A.1.1. Przekształcenia początkowe	243
A.1.2. Pętla główna MD5	244
A.1.3. Obliczenia końcowe	246
A.2. SHA-1	246
A.2.1. Przekształcenia początkowe	246
A.2.2. Pętla główna algorytmu SHA-1	247
A.2.3. Operacje w cyklu SHA-1	247
A.2.4. Obliczenia końcowe	248
A.3. SHA-2	249
A.3.1. Dodatkowe pojęcia	249
A.3.2. Przekształcenia początkowe	250
A.3.3. Operacje w cyklu SHA-2	251
A.3.4. Dodatkowe różnice między algorytmami SHA-2	253
A.4. SHA-3	254
A.4.1. SHA-3 — ogólny opis	254
A.4.2. Funkcja rundy SHA-3	254
A.4.3. Funkcja mieszająca SHA-3	256
A.5. Inne funkcje skrótu	257

Dodatek B Algorytmy szyfrujące 259

B.1. IDEA	259
B.1.1. Przekształcenia początkowe	259
B.1.2. Operacje pojedynczego cyklu IDEA	259
B.1.3. Generowanie podkluczy	261
B.1.4. Przekształcenia MA	261
B.1.5. Deszyfrowanie IDEA	261
B.2. DES	263
B.2.1. Permutacja początkowa (IP)	263
B.2.2. Podział tekstu na bloki	263

B.2.3. Permutacja rozszerzona	265
B.2.4. S-bloki	266
B.2.5. P-bloki	267
B.2.6. Permutacja końcowa	268
B.2.7. Deszyfrowanie DES	268
B.2.8. Modyfikacje DES	269
B.3. AES	271
B.3.1. Opis algorytmu	271
B.3.2. Generowanie kluczy	271
B.3.3. Pojedyncza runda algorytmu	272
B.3.4. Podsumowanie	274
B.4. Twofish	275
B.4.1. Opis algorytmu	275
B.4.2. Pojedyncza runda algorytmu	275
B.4.3. Podsumowanie	280
B.5. CAST5	280
B.5.1. Opis algorytmu	280
B.5.2. Rundy CAST5	281
B.6. Blowfish	282
B.6.1. Opis algorytmu	282
B.6.2. Funkcja algorytmu Blowfish	283
B.7. DSA	284
B.7.1. Podpisywanie wiadomości	284
B.7.2. Weryfikacja podpisu	285
B.7.3. Inne warianty DSA	285
B.8. RSA	287
B.8.1. Generowanie pary kluczy	287
B.8.2. Szyfrowanie i deszyfrowanie	287
B.9. Inne algorytmy szyfrujące	288
Dodatek C Kryptografia w służbie historii	291
C.1. Święte rysunki	292
C.1.1. 1000 lat później	293
C.1.2. Szyfr faraonów	294
C.1.3. Ziarno przeznaczenia	295
C.1.4. Je tiens l'affaire!	296
C.1.5. Tajemnica hieroglifów	297
C.2. Język mitów	298
C.2.1. Mit, który okazał się prawdziwy	298
C.2.2. Trojaczki Kober	301
C.2.3. Raport z półwiecza	303
C.3. Inne języki	305
Bibliografia	307
Skorowidz	309