

Spis treści

Przedmowa

9

1	Wprowadzenie	13
1.1	Kryptografia	13
1.2	Ochrona danych	16
1.3	Systemy kryptograficzne	20
1.3.1	Systemy klucza jawnego	25
1.3.2	Podpisy cyfrowe	28
1.4	Teoria informacji	30
1.4.1	Entropia i entropia warunkowa	31
1.4.2	Poufność doskonała	37
1.4.3	Długość krytyczna	40
1.5	Teoria złożoności	46
1.5.1	Złożoność algorytmu	46
1.5.2	Złożoność problemu i NP-zupełność	47
1.5.3	Szyfry oparte na problemach trudnych obliczeniowo	50
1.6	Teoria liczb	52
1.6.1	Kongruencje i arytmetyka modularna	52
1.6.2	Obliczanie odwrotności	56
1.6.3	Obliczenia w ciałach Galois	66
1.7	Ćwiczenia	71
	Literatura	73

2	Algorytmy szyfrowania	76
2.1	Szyfry przestawieniowe	76
2.2	Proste szyfry podstawieniowe	79
2.2.1	Analiza częstości występowania liter	82
2.3	Szyfry podstawieniowe homofoniczne	87
2.3.1	Szyfry Beale'a	88
2.3.2	Szyfry homofoniczne wyższych stopni	89
2.4	Szyfry podstawieniowe wieloalfabetyczne	90
2.4.1	Szyfry Vigenère'a i Beauforta	92
2.4.2	Wskaźnik zgodności	94
2.4.3	Metoda Kasiskiego	96
2.4.4	Szyfry z kluczem bieżącym	100

2.4.5	Maszyny rotorowe i maszyny Hagelina	102
2.4.6	Szyfr Vernama i szyfr z kluczem jednokrotnym	103
2.5	Szyfry poligramowe	105
2.5.1	Szyfr Playfaira	105
2.5.2	Szyfr Hilla	106
2.6	Szyfry kaskadowe	107
2.6.1	Szyfry podstawieniowo-permutacyjne	107
2.6.2	Szyfr DES	108
2.6.3	Uwarunkowania czasowo-pamięciowe	116
2.7	Szyfry wykładnicze	119
2.7.1	Szyfr Pohliga-Hallmana	121
2.7.2	Szyfr Rivesta-Shamira-Adlemana (RSA)	123
2.7.3	Gra w pokera na odległość	128
2.7.4	Przekazywanie sekretów	134
2.8	Szyfry plecakowe	137
2.8.1	Szyfr plecakowy Merklego-Hellmana	137
2.8.2	Szyfr plecakowy Grahama-Shamira	141
2.8.3	Szyfr plecakowy Shamira do kontroli tożsamości nadawcy	142
2.8.4	Przełamanywalny NP-zupełny szyfr plecakowy	145
2.9	Ćwiczenia	147
	Literatura	150

3

Techniki szyfrowania

3.1	Szyfry strumieniowe i blokowe	154
3.2	Synchroniczne szyfry strumieniowe	157
3.2.1	Liniowe rejestry przesuujące ze sprzężeniem zwrotnym	158
3.2.2	Tryb sprzężenia zwrotnego bloków wyjściowych	162
3.2.3	Metoda licznikowa	163
3.3	Samosynchronizujące się szyfry strumieniowe	164
3.3.1	Szyfry z automatycznym generowaniem klucza	164
3.3.2	Sprzężenie zwrotne zaszyfrowanego tekstu	165
3.4	Szyfry blokowe	167
3.4.1	Techniki wiązania bloków i wiązania bloków zaszyfrowanych	169
3.4.2	Szyfry blokowe z podkluczami	172
3.5	Węzły końcowe szyfrowania	175
3.5.1	Szyfrowanie w węzłach końcowych a szyfrowanie na poziomie połączeń	175
3.5.2	Homomorfizmy prywatności	179
3.6	Szyfry jednokierunkowe	183
3.6.1	Hasła dostępu a identyfikacja użytkownika	184
3.7	Zarządzanie kluczami	187
3.7.1	Klucze tajne	187
3.7.2	Klucze jawne	193
3.7.3	Generowanie kluczy dla szyfrów blokowych	195
3.7.4	Dystrybucja kluczy sesji	197
3.8	Metody progowe	204
3.8.1	Metoda wielomianu interpolacyjnego Lagrange'a	205
3.8.2	Metoda klas przystawiania	207
3.9	Ćwiczenia	210
	Literatura	212

4	Sterowanie dostępem	216
4.1	Model macierzy dostępu	217
4.1.1	Stan ochrony	217
4.1.2	Przejścia stanów	219
4.1.3	Polityki ochrony	225
4.2	Mechanizmy sterowania dostępem	225
4.2.1	Bezpieczeństwo i dokładność	225
4.2.2	Niezawodność i dzielenie zasobów	226
4.2.3	Zasady projektowania	230
4.3	Hierarchie dostępu	232
4.3.1	Tryby uprzywilejowane	232
4.3.2	Zagnieżdżone jednostki programu	233
4.4	Listy upoważnień	234
4.4.1	Obiekty własnościowe	235
4.4.2	Odwoływanie praw dostępu	238
4.5	Możliwości	241
4.5.1	Przełączanie domen z chronionymi punktami wejścia	243
4.5.2	Abstrakcyjne typy danych	244
4.5.3	Adresowanie oparte na możliwościach	249
4.5.4	Odwoływanie	252
4.5.5	Blokady i klucze	253
4.5.6	Modyfikacja zapytań	255
4.6	Systemy z weryfikowalną ochroną	256
4.6.1	Jądra ochrony (bezpieczeństwa)	257
4.6.2	Poziomy abstrakcji	260
4.6.3	Weryfikacja	262
4.7	Teoria systemów zaufanych	266
4.7.1	Systemy jednooperacyjne	267
4.7.2	Systemy ogólne	268
4.7.3	Teoria dla systemów ogólnych	271
4.7.4	Systemy typu <i>Brać-Dawać</i>	275
4.8	Ćwiczenia	284
	Literatura	286
5	Sterowanie przepływem danych	291
5.1	Model kratowy przepływu informacji	291
5.1.1	Polityka przepływu informacji	291
5.1.2	Stan informacyjny	292
5.1.3	Przejścia stanu a przepływ informacji	293
5.1.4	Struktura kraty	299
5.1.5	Właściwości przepływu krat	303
5.2	Mechanizmy sterowania przepływem	305
5.2.1	Bezpieczeństwo i dokładność	305
5.2.2	Kanały przepływu	307
5.3	Mechanizmy czasu wykonania	308
5.3.1	Dynamiczne wymuszanie bezpieczeństwa dla przepływów ukrytych	308
5.3.2	Sterowanie dostępem z przepływami bezpiecznymi	312
5.3.3	Maszyna do znakowania danych	315
5.3.4	Maszyna z jednym akumulatorem	317

5.4	Mechanizmy oparte na kompilacji	318
5.4.1	Specyfikacje przepływów	319
5.4.2	Wymagania bezpieczeństwa	321
5.4.3	Semantyki upoważniania	325
5.4.4	Ogólne struktury sterowania i danych	326
5.4.5	Współbieżność i synchronizacja	329
5.4.6	Nienormalne zakończenia	332
5.5	Weryfikacja programu	334
5.5.1	Instrukcja przypisania	336
5.5.2	Instrukcja złożona	338
5.5.3	Instrukcja warunkowa	338
5.5.4	Instrukcja iteracji	340
5.5.5	Instrukcja wywołania procedury	341
5.5.6	Bezpieczeństwo	344
5.6	Sterowanie przepływem w praktyce	346
5.6.1	Weryfikacja systemu	346
5.6.2	Rozszerzenia	349
5.6.3	System Guard	350
5.7	Ćwiczenia	352
	Literatura	356

6	Sterowanie wnioskowaniem	358
6.1	Model statystycznej bazy danych	358
6.1.1	Stan informacyjny	359
6.1.2	Rodzaje statystyk	360
6.1.3	Ujawnianie statystyk wrażliwych	363
6.1.4	Poufność całkowita i ochrona danych	366
6.1.5	Złożoność ujawniania	367
6.2	Mechanizmy sterowania wnioskowaniem	368
6.2.1	Bezpieczeństwo i dokładność	368
6.2.2	Metody udostępniania statystyk	369
6.3	Metody ataku	372
6.3.1	Atak z użyciem małych i dużych zbiorów odpowiedzi	372
6.3.2	Atak z użyciem szperaczy	374
6.3.3	Atak z użyciem układu równań liniowych	380
6.3.4	Atak medianą	385
6.3.5	Atak za pomocą wstawiania i usuwania rekordów	386
6.4	Mechanizmy ograniczania statystyk	387
6.4.1	Zabranianie komórek	389
6.4.2	Pytania implikowane	393
6.4.3	Podział bazy danych	398
6.5	Mechanizmy wprowadzające szумы	401
6.5.1	Zniekształcanie odpowiedzi (zaokrąglanie)	401
6.5.2	Losowanie zbioru odpowiedzi	404
6.5.3	Zniekształcanie danych	410
6.5.4	Wymiana danych	413
6.5.5	Odpowiedzi losowane (ankietowanie)	416
6.6	Podsumowanie	417
6.7	Ćwiczenia	418
	Literatura	420