

# Spis treści

O autorze .....	9
O recenzencie technicznym .....	9
Podziękowania .....	11
Wstęp .....	13

## **I** **SZYFROWANIE ..... 17**

Cel szyfrowania .....	18
Przestawianie — te same dane, różny porządek .....	19
Klucze szyfrów .....	20
Łamanie szyfrów .....	22
Podstawianie — zastępowanie danych .....	23
Zmienianie wzorca podstawiania .....	23
Poszerzanie klucza .....	25
Zaawansowany standard szyfrowania .....	26
Podstawy dwójkowe .....	27
Szyfrowanie AES w ujęciu ogólnym .....	29
Poszerzanie klucza w AES .....	30
Rundy szyfrowania AES .....	31
Łącuchowanie bloków .....	33
Dlaczego AES jest bezpieczny .....	33
Możliwe ataki na AES .....	35
Ograniczenia szyfrowania z kluczem symetrycznym .....	36

## **2** **HASŁA ..... 37**

Przekształcanie hasła w liczbę .....	38
Cechy dobrych funkcji haszowania .....	38
Funkcja skrótu MD5 .....	39
Kodowanie hasła .....	39
Operacje bitowe .....	40

Rundy haszowania MD5 .....	42
Spełnienie kryteriów dobrej funkcji haszowania .....	43
Podpisy cyfrowe .....	43
Problem tożsamości .....	44
Ataki z wykorzystaniem kolizji .....	44
Hasła w systemach uwierzytelniania .....	45
Zagrożenia dotyczące tablic haseł .....	45
Haszowanie haseł .....	46
Ataki słownikowe .....	47
Tablice haszowania .....	48
Łącuchowanie haszowania .....	48
Haszowanie iteracyjne .....	51
Solenie haseł .....	52
Czy tablice haseł są bezpieczne .....	53
Usługa przechowywania haseł .....	54
Przemyślenia końcowe .....	55

### 3

## **BEZPIECZEŃSTWO W SIECI ..... 57**

Jak kryptografia z kluczem publicznym rozwiązuje problem wspólnego klucza .....	58
Matematyczne narzędzia kryptografii z kluczem publicznym .....	59
Funkcje odwracalne .....	59
Funkcje jednokierunkowe .....	60
Funkcje z bocznym wejściem .....	60
Metoda szyfrowania RSA .....	63
Tworzenie kluczy .....	63
Szyfrowanie danych za pomocą RSA .....	65
Efektywność RSA .....	66
Zastosowanie szyfru RSA w rzeczywistym świecie .....	68
Użycie RSA do uwierzytelniania .....	71
Bezpieczeństwo w Sieci — protokół HTTPS .....	73
Wymiana potwierdzeń .....	74
Przesyłanie danych protokołem HTTPS .....	75
Czy problem wspólnego klucza został rozwiązany? .....	77

### 4

## **FILM CGI ..... 79**

Oprogramowanie tradycyjnej animacji .....	81
Jak działają obrazy cyfrowe .....	81
Sposoby definiowania kolorów .....	83
Jak oprogramowanie wykonuje animacje celuloidowe .....	84
Od oprogramowania animacji celuloidowej do renderowanej grafiki 2D .....	91
Oprogramowanie trójwymiarowej grafiki CGI .....	92
Jak opisuje się sceny trójwymiarowe .....	92
Kamera wirtualna .....	93

47	Oświetlenie bezpośrednie .....	93
48	Oświetlenie całego planu .....	98
49	Jak śledzić światło .....	99
50	Wygładzanie krawędzi w całej scenie .....	103
51	Łączenie rzeczywistego ze sztucznym .....	104
52	Ideał renderowania z jakością filmową .....	105

## 5

### **GRAFIKA GIER .....** **107**

53	Sprzęt do grafiki tworzonej w czasie rzeczywistym .....	108
54	Dlaczego w grach nie stosuje się śledzenia promieni .....	109
55	Same odcinki i żadnych krzywych .....	110
56	Rzutowanie bez śledzenia promieni .....	110
57	Renderowanie trójkątów .....	112
58	Algorytm malarza .....	113
59	Buforowanie głębokości .....	113
60	Oświetlanie w czasie rzeczywistym .....	115
61	Cienie .....	117
62	Światło otaczające i jego pochłanianie .....	118
63	Nanoszenie tekstur .....	120
64	Próbkowanie metodą najbliższego sąsiada .....	121
65	Filtrowanie dwuliniowe .....	123
66	Mipmapy .....	124
67	Filtrowanie trójliniowe .....	125
68	Odbicia .....	126
69	Fabrykowanie krzywizn .....	128
70	Oszukiwanie na dużych odległościach .....	129
71	Odzworowywanie wypukłości .....	129
72	Mozaikowanie .....	130
73	Wygładzanie krawędzi w czasie rzeczywistym .....	132
74	Superpróbkowanie .....	132
75	Wielopróbkowanie .....	134
76	Poprocesowe wygładzanie krawędzi .....	135
77	Budżet obrazowania .....	136
78	Co jeszcze w związku z grafiką gier .....	137

## 6

### **KOMPRESJA DANYCH .....** **139**

80	Kodowanie długości serii .....	141
81	Kompresja słownikowa .....	142
82	Podstawowa metoda .....	143
83	Kod Huffmana .....	144
84	Reorganizacja danych w celu lepszej kompresji .....	146
85	Kodowanie z przewidywaniem .....	146
86	Kwantyzacja .....	147

58	Obrazy w formacie JPEG .....	148
59	Inny sposób zapamiętywania kolorów .....	148
60	Dyskretna transformacja kosinusowa .....	149
61	DCT w dwóch wymiarach .....	152
62	Kompresowanie wyników .....	156
63	Jakość obrazów JPEG .....	159
64	Kompresja wideo wysokiej rozdzielczości .....	162
65	Nadmiarowość czasowa .....	162
66	Wideokompresja MPEG-2 .....	163
67	Jakość wideo z kompresją czasową .....	166
68	Teraźniejszość i przyszłość wideokompresji .....	168

## 7

### **WYSZUKIWANIE .....** 169

69	Zdefiniowanie problemu wyszukiwania .....	170
70	Porządkowanie danych .....	170
71	Sortowanie przez wybór .....	170
72	Sortowanie szybkie .....	171
73	Wyszukiwanie binarne .....	175
74	Indeksowanie .....	176
75	Haszowanie .....	178
76	Przeszukiwanie Sieci .....	181
77	Klasyfikacja wyników .....	182
78	Efektywne zastosowanie indeksów .....	184
79	Co dalej w związku z wyszukiwaniem w Sieci .....	185

## 8

### **WSPÓLBIEŻNOŚĆ .....** 187

80	Po co ta współbieżność? .....	187
81	Wydajność .....	188
82	Środowiska z wieloma użytkownikami .....	188
83	Wielozadaniowość .....	188
84	Kiedy współbieżność zawodzi .....	189
85	Jak działać współbieżnie i bezpiecznie .....	192
86	Dane tylko do czytania .....	192
87	Przetwarzanie transakcyjne .....	193
88	Semafor .....	194
89	Problem nieskończonego oczekiwania .....	196
90	Kolejki uporządkowane .....	196
91	Głodzenie wynikające z czekania cyklicznego .....	196
92	Kwestie sprawności semaforów .....	199
93	Co jeszcze w związku ze współbieżnością .....	200

<b>TRASY NA MAPACH .....</b>	<b>203</b>
Czym jest mapa w rozumieniu oprogramowania .....	203
Wyszukiwanie najpierw najlepszej .....	205
Ponowne wykorzystanie wcześniejszych wyników wyszukiwania .....	209
Jednoczesne znajdowanie wszystkich najlepszych tras .....	211
Algorytm Floyda .....	212
Zapamiętywanie kierunków tras .....	215
Przyszłość wytyczania tras .....	218
<b>SKOROWIDZ .....</b>	<b>219</b>

© referencje  
technicznym