
Spis treści

Wstęp	13
Jak czytać tę książkę	14

1.

Nasza filozofia projektowa	17
1.1. Zgubne skutki wydajności	17
1.2. Przekleństwa rozbudowanych możliwości	19

2.

Otoczka kryptografii	21
2.1. Rola kryptografii	21
2.2. Reguła najsłabszego ogniwa	22
2.3. Wizerunek przeciwnika	24
2.4. Myślenie paranoiczne	24
2.4.1. Atak	25
2.5. Model zagrożeń	26
2.6. Kryptografia nie rozwiązuje problemu	27
2.7. Kryptografia jest bardzo trudna	28
2.8. Kryptografia jest łatwym elementem systemu	28
2.9. Podstawowa literatura	29

3.

Wprowadzenie do kryptografii	31
3.1. Szyfrowanie	31
3.1.1. Zasada Kerckhoffs'a	32
3.2. Potwierdzanie tożsamości	33
3.3. Szyfrowanie z kluczem publicznym	34
3.4. Podpis cyfrowy	35
3.5. PKI	36

3.6. Ataki	37
3.6.1. Atak tylko z tekstem zaszyfrowanym	37
3.6.2. Atak ze znanym tekstem otwartym	37
3.6.3. Atak z wybranym tekstem otwartym	38
3.6.4. Atak z wybranym tekstem zaszyfrowanym	38
3.6.5. Rozróżnianie ataków	39
3.6.6. Atak urodzinowy	39
3.6.7. Spotkanie pośrodku	40
3.6.8. Inne rodzaje ataków	41
3.7. Poziom bezpieczeństwa	41
3.8. Wydajność	42
3.9. Złożoność	43

Część I Bezpieczeństwo komunikacji

45

4.

Szyfry blokowe	47
4.1. Co to jest szyfr blokowy?	47
4.2. Rodzaje ataku	48
4.3. Idealny szyfr blokowy	49
4.4. Definicja bezpieczeństwa szyfru blokowego	49
4.4.1. Parzystość permutacji	51
4.5. Praktyczne szyfry blokowe	52
4.5.1. DES	52
4.5.2. AES	55
4.5.3. Serpent	57
4.5.4. Twofish	58
4.5.5. Pozostali finaliści AES	59
4.5.6. Ataki przez rozwiązywanie równań	60
4.5.7. Którego szyfru blokowego należy użyć?	61
4.5.8. Jak długi powinien być mój klucz?	62

5.

Tryby szyfrów blokowych	63
5.1. Dopelnianie	63
5.2. ECB	64
5.3. CBC	65
5.3.1. Stały IV	65
5.3.2. IV jako licznik	65
5.3.3. Losowy IV	66
5.3.4. Jednorazowy IV	66
5.4. OFB	67
5.5. CTR	68
5.6. Nowe tryby	69
5.7. Którego trybu należy użyć?	70
5.8. Wycieki informacji	71
5.8.1. Prawdopodobieństwo kolizji	72
5.8.2. Jak radzić sobie z wyciekami	73
5.8.3. O naszym podejściu do matematyki	74

6.

Funkcje mieszające	75
6.1. Bezpieczeństwo funkcji mieszających	76
6.2. Prawdziwe funkcje mieszające	77
6.2.1. MD5	78
6.2.2. SHA-1	78
6.2.3. SHA-256, SHA-384 i SHA-512	79
6.3. Słabe punkty funkcji mieszających	79
6.3.1. Wydłużanie	80
6.3.2. Kolizja części wiadomości	80
6.4. Usuwanie słabych punktów	81
6.4.1. Rozwiązanie kompletne	81
6.4.2. Rozwiązanie wydajne	82
6.5. Wybór funkcji mieszającej	83
6.6. Ku przyszłości	84

7.

Kody uwierzytelniania wiadomości	85
7.1. Do czego służy MAC	85
7.2. Idealna funkcja MAC	85
7.3. Bezpieczeństwo MAC	86
7.4. CBC-MAC	87
7.5. HMAC	88
7.5.1. HMAC a SHA _d	89
7.6. UMAC	90
7.6.1. Rozmiar wyniku MAC	90
7.6.2. Która UMAC?	90
7.6.3. Elastyczność środowiska	91
7.6.4. Zakres analizy	92
7.6.5. Po co zatem w ogóle wspominać o UMAC?	92
7.7. Którą funkcję MAC wybrać?	92
7.8. Użycie funkcji MAC	93

8.

Bezpieczny kanał	95
8.1. Opis zagadnienia	95
8.1.1. Role	95
8.1.2. Klucz	96
8.1.3. Wiadomości czy strumień danych	96
8.1.4. Właściwości bezpieczeństwa	97
8.2. Kolejność potwierdzania wiarygodności i szyfrowania	98
8.3. Szkic rozwiązania	99
8.3.1. Numerowanie wiadomości	99
8.3.2. Potwierdzanie autentyczności	100
8.3.3. Szyfrowanie	101
8.3.4. Format ramki	101
8.4. Szczegóły implementacji	101
8.4.1. Inicjalizacja	102
8.4.2. Wysyłanie wiadomości	103

8.4.3. Odbieranie wiadomości.....	103
8.4.4. Kolejność wiadomości	105
8.5. Alternatywy	105
8.6. Podsumowanie.....	106

9.

O implementacji (I).....	107
9.1. Tworzenie poprawnych programów.....	108
9.1.1. Specyfikacje.....	108
9.1.2. Testowanie i poprawki	109
9.1.3. Lekceważące podejście	110
9.1.4. Co zatem robić?	110
9.2. Tworzenie bezpiecznego oprogramowania	111
9.3. Zachowywanie tajemnic	111
9.3.1. Kasowanie pamięci stanu.....	112
9.3.2. Plik wymiany	113
9.3.3. Pamięć podręczna	114
9.3.4. Zatrzymanie danych w pamięci.....	115
9.3.5. Dostęp osób postronnych.....	117
9.3.6. Integralność danych	117
9.3.7. Co robić	118
9.4. Jakość kodu źródłowego	118
9.4.1. Prostota	118
9.4.2. Modularyzacja.....	119
9.4.3. Asercje	120
9.4.4. Przpełnienie bufora	121
9.4.5. Testowanie	121
9.5. Ataki bocznym kanałem	122
9.6. Wnioski.....	123

Część II Negocjowanie kluczy

125

10.

Generowanie wartości losowych	127
10.1. Wartości prawdziwie losowe	128
10.1.1. Problemy związane z użyciem prawdziwych danych losowych	128
10.1.2. Dane pseudolosowe	129
10.1.3. Prawdziwe dane losowe i PRNG	129
10.2. Modele ataku na PRNG	130
10.3. Fortuna.....	131
10.4. Generator	131
10.4.1. Inicjalizacja.....	133
10.4.2. Ponowne przekazanie ziarna	133
10.4.3. Generowanie bloków	133
10.4.4. Generowanie danych losowych.....	134
10.4.5. Szybkość działania generatora	135
10.5. Akumulator.....	135
10.5.1. Źródła entropii	135
10.5.2. Pule	136
10.5.3. O implementacji.....	137

10.5.4. Inicjalizacja.....	139
10.5.5. Pobieranie losowych danych.....	140
10.5.6. Dodawanie zdarzenia.....	141
10.6. Obsługa pliku ziarna.....	142
10.6.1. Zapis pliku ziarna.....	142
10.6.2. Aktualizacja pliku ziarna.....	142
10.6.3. Kiedy czytać i zapisywać plik ziarna.....	143
10.6.4. Kopie bezpieczeństwa.....	143
10.6.5. Atomowość aktualizacji w systemie plików.....	144
10.6.6. Pierwsze uruchomienie.....	144
10.7. Co zatem robić?.....	145
10.8. Dobieranie elementów losowych.....	145

11.

Liczby pierwsze.....	147
11.1. Podzielność i liczby pierwsze.....	147
11.2. Generowanie małych liczb pierwszych.....	149
11.3. Operacje arytmetyczne modulo liczba pierwsza.....	150
11.3.1. Dodawanie i odejmowanie.....	151
11.3.2. Mnożenie.....	151
11.3.3. Ciała skończone i grupy.....	151
11.3.4. Algorytm NWD.....	152
11.3.5. Rozszerzony algorytm Euklidesa.....	153
11.3.6. Działania modulo 2.....	154
11.4. Duże liczby pierwsze.....	155
11.4.1. Testowanie pierwszości.....	157
11.4.2. Potęgowanie.....	159

12.

Diffie-Hellman.....	161
12.1. Grupy.....	161
12.2. Wersja podstawowa DH.....	162
12.3. Man-in-the-middle.....	163
12.4. Pułapki.....	164
12.5. Bezpieczne liczby pierwsze.....	165
12.6. Używanie mniejszej podgrupy.....	166
12.7. Rozmiar p.....	167
12.8. Zasady praktyczne.....	168
12.9. Co może się nie udać?.....	169

13.

RSA.....	171
13.1. Wprowadzenie.....	171
13.2. Chińskie twierdzenie o resztach.....	171
13.2.1. Wzór Garnera.....	172
13.2.2. Uogólnienia.....	173
13.2.3. Zastosowania.....	173
13.2.4. Wnioski.....	174

13.3. Mnożenie modulo n	174
13.4. Definicja RSA	175
13.4.1. RSA i podpisy cyfrowe	175
13.4.2. Wykładniki publiczne	176
13.4.3. Klucz prywatny	176
13.4.4. Wielkość n	177
13.4.5. Generowanie kluczy RSA	178
13.5. Pułapki związane z użyciem RSA	179
13.6. Szyfrowanie	180
13.7. Podpisy	182

14.

Wprowadzenie do protokołów kryptograficznych	185
14.1. Role	185
14.2. Zaufanie	185
14.2.1. Ryzyko	187
14.3. Motywacje	187
14.4. Zaufanie w protokołach kryptograficznych	189
14.5. Wiadomości i etapy	189
14.5.1. Warstwa nośna (transportowa)	189
14.5.2. Tożsamość protokołu i wiadomości	190
14.5.3. Kodowanie i analiza wiadomości	191
14.5.4. Stany wykonania protokołu	191
14.5.5. Błędy	192
14.5.6. Powtórki i ponowne próby	193

15.

Protokół negocjacji klucza	195
15.1. Otoczenie	195
15.2. Pierwsze podejście	196
15.3. Protokoły są wieczne	197
15.4. Konwencja potwierdzania autentyczności	197
15.5. Drugie podejście	198
15.6. Trzecie podejście	199
15.7. Ostateczna postać protokołu	199
15.8. Różne spojrzenia na protokół	202
15.8.1. Punkt widzenia Alicji	202
15.8.2. Punkt widzenia Boba	202
15.8.3. Punkt widzenia atakującego	202
15.8.4. Ujawnienie klucza	203
15.9. Złożoność obliczeniowa protokołu	204
15.9.1. Sztuczki optymalizacyjne	205
15.10. Złożoność protokołu	205
15.11. Małe ostrzeżenie	206
15.12. Negocjacja klucza na podstawie hasła	206

16.

O implementacji (II)	209
16.1. Arytmetyka dużych liczb całkowitych	209
16.1.1. Wooping	210
16.1.2. Sprawdzanie obliczeń DH	212
16.1.3. Sprawdzanie szyfrowania RSA	213
16.1.4. Sprawdzanie podpisów RSA	213
16.1.5. Wnioski	213
16.2. Przyspieszenie mnożenia	214
16.3. Ataki bocznym kanałem	215
16.3.1. Środki zaradcze	215
16.4. Protokoły	216
16.4.1. Protokoły w bezpiecznym kanale	217
16.4.2. Odbieranie komunikatów	217
16.4.3. Brak odpowiedzi w zadanym czasie	218

Część III Zarządzanie kluczami

219

17.

Zegar	221
17.1. Zastosowania zegara	221
17.1.1. Utrata ważności	221
17.1.2. Niepowtarzalne wartości	221
17.1.3. Monotoniczność	222
17.1.4. Transakcje w czasie rzeczywistym	222
17.2. Użycie sprzętowego zegara	223
17.3. Zagrożenia dla bezpieczeństwa	223
17.3.1. Cofnięcie zegara	223
17.3.2. Zatrzymanie zegara	224
17.3.3. Przeszycie zegara w przód	224
17.4. Budowa niezawodnego zegara	225
17.5. Problem takiego samego stanu	226
17.6. Czas	227
17.7. Wnioski	228

18.

Serwery kluczy	229
18.1. Podstawy	229
18.2. Kerberos	230
18.3. Prostsze rozwiązania	230
18.3.1. Bezpieczne połączenie	231
18.3.2. Przygotowanie klucza	231
18.3.3. Zmiana klucza	232
18.3.4. Inne właściwości	232
18.4. Jak dokonać wyboru	232

19.

Marzenia o PKI	233
19.1. Krótkie wprowadzenie do PKI.....	233
19.2. Przykładowy PKI.....	234
19.2.1. Uniwersalne PKI.....	234
19.2.2. Dostęp VPN.....	234
19.2.3. Bankowość elektroniczna	234
19.2.4. Czujniki w rafinerii.....	234
19.2.5. Centrum kart kredytowych.....	235
19.3. Dodatkowe szczegóły	235
19.3.1. Certyfikaty wielopoziomowe.....	235
19.3.2. Wygasanie certyfikatów.....	236
19.3.3. Osobny podmiot rejestrujący	236
19.4. Wnioski.....	237

20.

Rzeczywistość PKI	239
20.1. Nazwy	239
20.2. Podmiot decydujący.....	241
20.3. Zaufanie.....	241
20.4. Autoryzacja pośrednia	242
20.5. Autoryzacja bezpośrednia.....	242
20.6. Systemy delegacji uprawnień.....	243
20.7. Marzenie po modyfikacjach.....	244
20.8. Odbieranie uprawnień.....	245
20.8.1. Lista odwołań.....	245
20.8.2. Krótki okres ważności.....	246
20.8.3. Odwoływanie jest potrzebne.....	246
20.9. Do czego naprawdę służy PKI?	247
20.10. Co wybrać.....	248

21.

PKI w praktyce	249
21.1. Format certyfikatu.....	249
21.1.1. Język uprawnień.....	249
21.1.2. Klucz główny	250
21.2. Cykl życia klucza.....	250
21.3. Czemu klucze się zużywają	252
21.4. Co zatem zrobić?	253

22.

Przechowywanie tajemnic	255
22.1. Dysk.....	255
22.2. Pamięć ludzka.....	256
22.2.1. Solenie i rozciąganie	257
22.3. Pamięć przenośna	258
22.4. Token bezpieczeństwa	259

22.5. Bezpieczny interfejs użytkownika	260
22.6. Dane biometryczne	260
22.7. Jednorazowa rejestracja	261
22.8. Ryzyko utraty.....	262
22.9. Wspólne tajemnice.....	262
22.10. Usuwanie tajemnic.....	263
22.10.1. Papier	263
22.10.2. Pamięć magnetyczna.....	263
22.10.3. Pamięci trwale.....	264

Część IV Różności **265**

23.

Standardy	267
23.1. Proces tworzenia standardów.....	267
23.1.1. Standard.....	268
23.1.2. Funkcjonalność	268
23.1.3. Bezpieczeństwo.....	269
23.2. SSL	269
23.3. AES: standaryzacja w wyniku konkursu.....	270

24.

Patenty.....	271
24.1. Stan zastany	271
24.2. Kontynuacje.....	272
24.3. Niepewność.....	272
24.4. Czytanie patentów.....	272
24.5. Licencjonowanie.....	273
24.6. Patenty ochronne	274
24.7. Naprawa systemu patentowego.....	274
24.8. Nota prawna.....	275

25.

Pomoc ekspertów	277
-----------------------	-----

Dodatki **281**

Bibliografia	283
Skorowidz	289