
Spis treści

Wstęp	XI
1 Wprowadzenie do kryptografii	1
1.1 Kryptosystemy i podstawowe narzędzia kryptograficzne	1
1.1.1 Kryptosystemy z kluczem tajnym	1
1.1.2 Kryptosystemy klucza publicznego	2
1.1.3 Szyfry blokowe i strumieniowe	3
1.1.4 Kryptografia hybrydowa	3
1.2 Integralność wiadomości	4
1.2.1 Kody uwierzytelniania wiadomości	5
1.2.2 Schematy podpisów	6
1.2.3 Niezaprzeczalność	7
1.2.4 Certyfikaty	7
1.2.5 Funkcje skrótów	8
1.3 Protokoły kryptograficzne	9
1.4 Bezpieczeństwo	10
1.5 Uwagi i źródła	13
2 Klasyczna kryptografia	14
2.1 Wprowadzenie: niektóre proste kryptosystemy	14
2.1.1 Szyfr przestawieniowy	16
2.1.2 Szyfr podstawieniowy	19
2.1.3 Szyfr afiniczny	20
2.1.4 Szyfr Vigenère’a	25
2.1.5 Szyfr Hilla	26
2.1.6 Szyfr permutacyjny	31
2.1.7 Szyfry strumieniowe	33
2.2 Kryptoanaliza	37
2.2.1 Kryptoanaliza szyfru afinicznego	39
2.2.2 Kryptoanaliza szyfru podstawieniowego	40
2.2.3 Kryptoanaliza szyfru Vigenère’a	43
2.2.4 Kryptoanaliza szyfru Hilla	47
2.2.5 Kryptoanaliza szyfru strumieniowego z LFSR	48
2.3 Uwagi i źródła	49
Ćwiczenia	50

3	Teoria Shannona, tajność doskonała i szyfr z kluczem jednorazowym	57
3.1	Wprowadzenie	57
3.2	Podstawowa teoria prawdopodobieństwa	58
3.3	Tajność doskonała	61
3.4	Entropia	66
3.4.1	Cechy entropii	68
3.5	Fałszywe klucze i długość krytyczna	71
3.6	Uwagi i źródła	75
	Ćwiczenia	76
4	Szyfry blokowe i szyfry strumieniowe	79
4.1	Wprowadzenie	79
4.2	Sieci podstawieniowo-permutacyjne	80
4.3	Kryptoanaliza liniowa	85
4.3.1	Lemat nawarstwiania	85
4.3.2	Liniowe aproksymacje S-boksów	87
4.3.3	Liniowy atak na SPN	90
4.4	Kryptoanaliza różnicowa	94
4.5	Data Encryption Standard	101
4.5.1	Opis DES	101
4.5.2	Analiza DES	103
4.6	Advanced Encryption Standard	105
4.6.1	Opis AES	106
4.6.2	Analiza AES	111
4.7	Tryby działania	112
4.7.1	Atak wyroczni dopełnienia w trybie CBC	116
4.8	Szyfry strumieniowe	118
4.8.1	Atak korelacyjny na generator kombinacji	119
4.8.2	Atak algebraiczny na generator filtrów	122
4.8.3	Trivium	125
4.9	Uwagi i źródła	126
	Ćwiczenia	127
5	Funkcje skrótu i uwierzytelnianie wiadomości	132
5.1	Funkcje skrótu i integralność danych	132
5.2	Bezpieczeństwo funkcji skrótu	134
5.2.1	Model losowej wyroczni	136
5.2.2	Algorytmy w modelu losowej wyroczni	137
5.2.3	Porównanie kryteriów bezpieczeństwa	141
5.3	Iterowane funkcje skrótu	144
5.3.1	Konstrukcja Merkle'a–Damgåarda	146
5.3.2	Kilka przykładów iterowanych funkcji skrótów	151
5.4	Konstrukcja gąbki	152
5.4.1	SHA-3	155
5.5	Kody uwierzytelniania wiadomości	156
5.5.1	Zagnieżdżone kody MAC i HMAC	158
5.5.2	CBC-MAC	161
5.5.3	Szyfrowanie uwierzytelnione	162

5.6	Bezwarunkowo bezpieczne kody MAC	165
5.6.1	Silnie uniwersalne rodziny skrótów	168
5.6.2	Optymalność prawdopodobieństwa oszustwa	170
5.7	Uwagi i źródła	172
	Ćwiczenia	173
6	Kryptosystem RSA i rozkład liczb całkowitych na czynniki	181
6.1	Wprowadzenie do kryptografii klucza publicznego	181
6.2	Więcej teorii liczb	184
6.2.1	Algorytm Euklidesa	184
6.2.2	Chińskie twierdzenie o resztach	188
6.2.3	Inne przydatne fakty	190
6.3	Kryptosystem RSA	192
6.3.1	Implementowanie RSA	194
6.4	Testowanie pierwszości	197
6.4.1	Symbole Legendre’a i Jacobiego	199
6.4.2	Algorytm Solovaya–Strassena	202
6.4.3	Algorytm Millera–Rabina	205
6.5	Pierwiastki kwadratowe modulo n	207
6.6	Algorytmy rozkładu na czynniki	208
6.6.1	Algorytm Pollarda $p - 1$	209
6.6.2	Algorytm rho Pollarda	210
6.6.3	Algorytm losowych kwadratów Dixona	213
6.6.4	Algorytmy rozkładu na czynniki w praktyce	218
6.7	Inne ataki na RSA	219
6.7.1	Obliczanie $\varphi(n)$	220
6.7.2	Wykładnik odszyfrowywania	220
6.7.3	Atak Wienera z małym wykładnikiem odszyfrowywania	225
6.8	Kryptosystem Rabina	229
6.8.1	Bezpieczeństwo kryptosystemu Rabina	231
6.9	Bezpieczeństwo semantyczne RSA	233
6.9.1	Częściowe informacje dotyczące bitów tekstu jawnego	234
6.9.2	Uzyskanie bezpieczeństwa semantycznego	236
6.10	Uwagi i źródła	241
	Ćwiczenia	242
7	Kryptografia klucza publicznego i logarytmy dyskretne	251
7.1	Wprowadzenie	251
7.1.1	Kryptosystem ElGamala	252
7.2	Algorytmy dla problemu logarytmu dyskretnego	254
7.2.1	Algorytm Shanksa	254
7.2.2	Algorytm logarytmu dyskretnego rho Pollarda	256
7.2.3	Algorytm Pohliga–Hellmana	259
7.2.4	Metoda rachunku indeksowego	262
7.3	Dolne granice złożoności algorytmów generycznych	264
7.4	Ciała skończone	268
7.4.1	Analiza indeksu Joux’a dla ciał o niewielkich wyróżnikach	272

7.5	Krzywe eliptyczne	274
7.5.1	Krzywe eliptyczne na liczbach rzeczywistych	274
7.5.2	Krzywe eliptyczne modulo liczba pierwsza	277
7.5.3	Krzywe eliptyczne na ciałach skończonych	280
7.5.4	Własności krzywych eliptycznych	281
7.5.5	Parowanie krzywych eliptycznych	282
7.5.6	Kryptosystem ElGamala na krzywych eliptycznych	285
7.5.7	Obliczanie wielokrotności punktów na krzywych eliptycznych	287
7.6	Algorytmy logarytmu dyskretnego w praktyce	290
7.7	Bezpieczeństwo systemów ElGamala	291
7.7.1	Bitowe bezpieczeństwo logarytmów dyskretnych	291
7.7.2	Semantyczne bezpieczeństwo systemów ElGamala	295
7.7.3	Problemy Diffiego–Hellmana	295
7.8	Uwagi i źródła	297
	Ćwiczenia	298
8	Schematy podpisów	304
8.1	Wprowadzenie	304
8.1.1	Schemat podpisu RSA	305
8.2	Wymogi bezpieczeństwa dla schematów podpisu	307
8.2.1	Podpisy i funkcje skrótu	308
8.3	Schemat podpisu ElGamala	309
8.3.1	Bezpieczeństwo schematu podpisu ElGamala	312
8.4	Warianty schematu podpisu ElGamala	315
8.4.1	Schemat podpisu Schnorra	315
8.4.2	Algorytm podpisu cyfrowego	317
8.4.3	DSA krzywej eliptycznej	319
8.5	Funkcja skrótu o pełnej dziedzinie	321
8.6	Certyfikaty	325
8.7	Podpisywanie i szyfrowanie	326
8.8	Uwagi i źródła	328
	Ćwiczenia	329
9	Kryptografia postkwantowa	334
9.1	Wprowadzenie	334
9.2	Kryptografia oparta na kratkach	337
9.2.1	NTRU	337
9.2.2	Kraty i bezpieczeństwo NTRU	341
9.2.3	LWE	344
9.3	Kryptografia oparta na kodzie i kryptosystem McEliece’a	346
9.4	Kryptografia wielu zmiennych	351
9.4.1	Równania ciała ukrytego	352
9.4.2	Schemat podpisu oliwa i ocet	356
9.5	Schematy podpisu oparte na skrócie	360
9.5.1	Schemat podpisu Lamporta	360
9.5.2	Schemat podpisu Winternitza	362
9.5.3	Schemat podpisu Merkle’a	365
9.6	Uwagi i źródła	367
	Ćwiczenia	368

10	Schematy identyfikacji i uwierzytelnianie jednostki	370
10.1	Wprowadzenie	370
10.1.1	Hasła	372
10.1.2	Bezpieczne schematy identyfikacji	374
10.2	Wyzwanie i odpowiedź w kryptografii klucza tajnego	375
10.2.1	Model ataku i cele przeciwnika	380
10.2.2	Wzajemne uwierzytelnianie	382
10.3	Wyzwanie i odpowiedź dla kryptografii klucza publicznego	385
10.3.1	Schematy identyfikacji klucza publicznego	385
10.4	Schemat identyfikacji Schnorra	388
10.4.1	Bezpieczeństwo schematu identyfikacji Schnorra	391
10.5	Schemat identyfikacji Feige’a–Fiata–Shamira	397
10.6	Uwagi i źródła	402
	Ćwiczenia	402
11	Dystrybucja kluczy	406
11.1	Wprowadzenie	406
11.1.1	Modele ataku i cele przeciwników	409
11.2	Wstępna dystrybucja kluczy	410
11.2.1	Wstępna dystrybucja kluczy Diffiego–Hellmana	410
11.2.2	Schemat Bloma	412
11.2.3	Wstępna dystrybucja klucza w sieciach czujnikowych	419
11.3	Schematy dystrybucji klucza sesji	423
11.3.1	Schemat Needhama–Schroedera	423
11.3.2	Atak Denninga–Sacca na schemat NS	424
11.3.3	Kerberos	426
11.3.4	Schemat Bellare’a–Rogawaya	429
11.4	Ponowne tworzenie klucza i logiczna hierarchia kluczy	432
11.5	Schematy progowe	435
11.5.1	Schemat Shamira	436
11.5.2	Uproszczony schemat (t, t) -progowy	439
11.5.3	Wizualne schematy progowe	440
11.6	Uwagi i źródła	444
	Ćwiczenia	444
12	Schematy uzgadniania klucza	450
12.1	Wprowadzenie	450
12.1.1	Bezpieczeństwo warstwy transportu (TLS)	450
12.2	Uzgodnienie klucza Diffiego–Hellmana	452
12.2.1	Schemat uzgadniania klucza STS (station-to-station)	454
12.2.2	Bezpieczeństwo STS	455
12.2.3	Ataki ze znanym kluczem sesji	458
12.3	Funkcje wyprowadzania klucza	460
12.4	Schematy MTI uzgadniania klucza	462
12.4.1	Ataki na MTI/A0 ze znanym kluczem sesji	464
12.5	Zaprzeczone schematy uzgadniania klucza	466

12.6	Aktualizacja kluczy	469
12.7	Konferencyjne schematy uzgadniania klucza	472
12.8	Uwagi i źródła	475
	Ćwiczenia	475
13	Różne tematy	478
13.1	Kryptografia oparta na tożsamości	478
13.1.1	Kryptosystem Cocksza oparty na tożsamości	479
13.1.2	Kryptosystem Boneha–Franklina oparty na tożsamości	485
13.2	Kryptosystem Pailliera	490
13.3	Ochrona praw autorskich	493
13.3.1	Odciski palca	494
13.3.2	Identyfikowalna własność nadrzędna	496
13.3.3	Kody 2-IPP	498
13.3.4	Śledzenie nielegalnej redystrybucji kluczy	501
13.4	Bitcoin i technologia blockchain	505
13.5	Uwagi i źródła	509
	Ćwiczenia	510
A	Teoria liczb i algebraiczne koncepcje kryptografii	513
A.1	Arytmetyka modularna	513
A.2	Grupy	514
A.2.1	Rzędy elementów grupy	516
A.2.2	Grupy cykliczne i elementy pierwotne	517
A.2.3	Podgrupy i warstwy	518
A.2.4	Izomorfizmy i homomorfizmy grup	519
A.2.5	Reszty kwadratowe	520
A.2.6	Algorytm Euklidesa	521
A.2.7	Iloczyny proste	522
A.3	Pierścienie	523
A.3.1	Chińskie twierdzenie o resztach	524
A.3.2	Ideały i pierścienie ilorazowe	526
A.4	Ciała	527
B	Pseudolosowe generowanie bitów dla kryptografii	530
B.1	Generatory bitów	530
B.2	Bezpieczeństwo pseudolosowych generatorów bitów	535
B.3	Uwagi i źródła	537
	Bibliografia	538
	Indeks	548