

SPIS TREŚCI

Notacja 11

Przedmowa 13

O autorze 23

Rozdział 0. Przewodnik po treści 25

- 0.1. Układ książki 26
- 0.2. Wskazówki dla czytelników i instruktorów 27
- 0.3. Zasoby internetowe 29
- 0.4. Standardy 31

Rozdział 1. Ogólny zarys bezpieczeństwa komputerowego 33

- 1.1. Koncepcje bezpieczeństwa komputerowego 36
- 1.2. Architektura bezpieczeństwa OSI 42
- 1.3. Ataki na bezpieczeństwo 43
- 1.4. Usługi bezpieczeństwa 45
- 1.5. Mechanizmy bezpieczeństwa 51
- 1.6. Model bezpieczeństwa sieci 51
- 1.7. Zalecane materiały uzupełniające 55
- 1.8. Kluczowe terminy, pytania przeglądowe i problemy 57

CZĘŚĆ I SZYFRY SYMETRYCZNE 61

Rozdział 2. Klasyczne techniki szyfrowania 61

- 2.1. Model szyfrowania symetrycznego 63
- 2.2. Techniki podstawieniowe 70
- 2.3. Techniki przestawieniowe 88
- 2.4. Maszyny wirnikowe 89
- 2.5. Steganografia 91
- 2.6. Zalecane materiały uzupełniające 94
- 2.7. Kluczowe terminy, pytania przeglądowe i problemy 95

Rozdział 3. Szyfry blokowe i standard DES 103

- 3.1. Podstawowe cechy szyfru blokowego 105
- 3.2. Standard DES 115
- 3.3. Przykład 124
- 3.4. Siła szyfru DES 127
- 3.5. Kryptoanaliza różnicowa i kryptoanaliza liniowa 129
- 3.6. Zasady projektowania szyfrów blokowych 133

3.7.	Zalecane materiały uzupełniające	138
3.8.	Kluczowe terminy, pytania przeglądowe i problemy	139
Rozdział 4. Podstawy teorii liczb i ciał skończonych 145		
4.1.	Podzielność i algorytm dzielenia	147
4.2.	Algorytm Euklidesa	149
4.3.	Arytmetyka modularna	152
4.4.	Grupy, pierścienie i ciała	162
4.5.	Ciała skończone postaci $GF(p)$	166
4.6.	Arytmetyka wielomianowa	170
4.7.	Ciała skończone postaci $GF(2^n)$	177
4.8.	Zalecane materiały uzupełniające	189
4.9.	Kluczowe terminy, pytania przeglądowe i problemy	190
	Dodatek 4A. Znaczenie operatora mod	194
Rozdział 5. Standard AES 197		
5.1.	Arytmetyka ciał skończonych	198
5.2.	Struktura AES	200
5.3.	Funkcje transformacyjne AES	206
5.4.	Rozwijanie klucza	218
5.5.	Przykład zastosowania AES	220
5.6.	Implementacja AES	224
5.7.	Zalecane materiały uzupełniające	231
5.8.	Kluczowe terminy, pytania przeglądowe i problemy	231
	Dodatek 5A. Wielomiany o współczynnikach z $GF(2^8)$	233
	Dodatek 5B. Uproszczony szyfr AES (S-AES)	236
Rozdział 6. Tryby operacyjne szyfrów blokowych 247		
6.1.	Wielokrotne szyfrowanie i potrójny DES	248
6.2.	Tryb elektronicznej książki kodowej	254
6.3.	Łącuchowanie bloków szyfrogramu	257
6.4.	Sprzężenie zwrotne szyfrogramu	259
6.5.	Sprzężenie wyjściowe	261
6.6.	Tryb licznikowy	263
6.7.	Tryb XTS-AES dla urządzeń blokowych o orientacji sektorowej	266
6.8.	Polecana strona WWW	271
6.9.	Kluczowe terminy, pytania przeglądowe i problemy	272
Rozdział 7. Generatory liczb pseudolosowych i szyfry strumieniowe 277		
7.1.	Zasady generowania liczb pseudolosowych	278
7.2.	Generatory liczb pseudolosowych	286
7.3.	Generowanie liczb pseudolosowych na bazie szyfrów blokowych	289
7.4.	Szyfry strumieniowe	293
7.5.	RC4	295
7.6.	Generatory liczb prawdziwie losowych	297

7.7.	Zalecane materiały uzupełniające	300
7.8.	Kluczowe terminy, pytania przeglądowe i problemy	302
CZĘŚĆ II	SZYFRY ASYMETRYCZNE	307
Rozdział 8.	Wstęp do teorii liczb	307
8.1.	Liczby pierwsze	309
8.2.	Twierdzenia Fermata i Eulera	312
8.3.	Testowanie, czy liczba jest pierwsza	316
8.4.	Chińskie twierdzenie o resztach	320
8.5.	Logarytmy dyskretne	322
8.6.	Zalecane materiały uzupełniające	328
8.7.	Kluczowe terminy, pytania przeglądowe i problemy	329
Rozdział 9.	Kryptografia z kluczami publicznymi i szyfr RSA	333
9.1.	Zasady funkcjonowania kryptosystemów z kluczami publicznymi	336
9.2.	Algorytm RSA	346
9.3.	Zalecane materiały uzupełniające	361
9.4.	Kluczowe terminy, pytania przeglądowe i problemy	363
	Dodatek 9A. Dowód poprawności algorytmu RSA	368
	Dodatek 9B. Złożoność algorytmów	370
Rozdział 10.	Inne systemy kryptografii z kluczami publicznymi	375
10.1.	Algorytm Diffiego-Hellmana wymiany kluczy	377
10.2.	System kryptograficzny ElGamal	381
10.3.	Arytmetyka krzywych eliptycznych	384
10.4.	Kryptografia krzywych eliptycznych	394
10.5.	Generatory liczb pseudolosowych bazujące na szyfrach asymetrycznych	397
10.6.	Zalecane materiały uzupełniające	400
10.7.	Kluczowe terminy, pytania przeglądowe i problemy	401
CZĘŚĆ III	KRYPTOGRAFICZNE ALGORYTMY OCHRONY INTEGRALNOŚCI DANYCH	405
Rozdział 11.	Kryptograficzne funkcje haszujące	405
11.1.	Zastosowania kryptograficznych funkcji haszujących	407
11.2.	Dwie proste funkcje haszujące	411
11.3.	Wymagania stawiane funkcjom haszującym	414
11.4.	Funkcje haszujące bazujące na łańcuchowaniu szyfrogramów	422
11.5.	Algorytmy rodziny SHA	423
11.6.	SHA-3	433
11.7.	Zalecane materiały uzupełniające	434
11.8.	Kluczowe terminy, pytania przeglądowe i problemy	435
	Dodatek 11A. Matematyczne podstawy paradoksu urodzin	439

Rozdział 12. Uwierzytelnianie komunikatów 447

- 12.1. Wymagania stawiane uwierzytelnianiu komunikatów 449
- 12.2. Funkcje wykorzystywane do uwierzytelniania komunikatów 450
- 12.3. Wymagania stawiane kodom uwierzytelniania komunikatów 458
- 12.4. Bezpieczeństwo kodów uwierzytelniania komunikatów 461
- 12.5. Uwierzytelnianie komunikatów oparte na haszowaniu 463
- 12.6. Uwierzytelnianie komunikatów bazujące na szyfrach blokowych: DAA i CMAC 468
- 12.7. Uwierzytelniane szyfrowanie: CCM i GCM 472
- 12.8. Generowanie liczb pseudolosowych za pomocą haszowania i kodów MAC 479
- 12.9. Zalecane materiały uzupełniające 482
- 12.10. Kluczowe terminy, pytania przeglądowe i problemy 483

Rozdział 13. Podpisy cyfrowe 487

- 13.1. Podpisy cyfrowe 489
- 13.2. Podpisy cyfrowe ElGamal 493
- 13.3. Schemat Schnorra podpisu cyfrowego 495
- 13.4. Standard DSS 496
- 13.5. Zalecane materiały uzupełniające 499
- 13.6. Kluczowe terminy, pytania przeglądowe i problemy 500

DODATKI 505**Dodatek A Projekty dydaktyczne 505**

- A.1. System algebry komputerowej Sage 506
- A.2. Projekt hackingu 507
- A.3. Projekty związane z szyframi blokowymi 508
- A.4. Ćwiczenia laboratoryjne 508
- A.5. Projekty poszukiwawcze 509
- A.6. Zadania programistyczne 509
- A.7. Praktyczna ocena bezpieczeństwa 510
- A.8. Wypracowania pisemne 510
- A.9. Lektura tematu 511

Dodatek B Przykłady dla systemu Sage 513

- B.1. Algebra liniowa i operacje na macierzach 514
- B.2. Rozdział 2. — klasyczne techniki szyfrowania 515
- B.3. Rozdział 3. — szyfry blokowe i standard DES 518
- B.4. Rozdział 4. — podstawy teorii liczb i ciał skończonych 521
- B.5. Rozdział 5. — standard AES 526
- B.6. Rozdział 7. — generatory liczb pseudolosowych i szyfry strumieniowe 530
- B.7. Rozdział 8. — teoria liczb 532
- B.8. Rozdział 9. — kryptografia z kluczami publicznymi i szyfr RSA 536
- B.9. Rozdział 10. — inne systemy kryptografii z kluczami publicznymi 539
- B.10. Rozdział 11. — kryptograficzne funkcje haszujące 544
- B.11. Rozdział 13. — podpisy cyfrowe 545

Dodatek C	Ćwiczenia z systemem Sage	549
C.1.	Sage — pierwszy kontakt	550
C.2.	Programowanie w Sage	552
C.3.	Rozdział 2. — klasyczne techniki szyfrowania	558
C.4.	Rozdział 3. — szyfry blokowe i standard DES	559
C.5.	Rozdział 4. — podstawy teorii liczb i ciał skończonych	560
C.6.	Rozdział 5. — standard AES	562
C.7.	Rozdział 7. — generatory liczb pseudolosowych i szyfry strumieniowe	565
C.8.	Rozdział 8. — teoria liczb	566
C.9.	Rozdział 9. — kryptografia z kluczami publicznymi i szyfr RSA	570
C.10.	Rozdział 10. — inne systemy kryptografii z kluczami publicznymi	571
C.11.	Rozdział 11. — kryptograficzne funkcje haszujące	574
C.12.	Rozdział 13. — podpisy cyfrowe	575
Dodatek D	Standardy i organizacje standaryzacyjne	577
D.1.	Znaczenie standardów	578
D.2.	Standardy internetowe i społeczność internetu	579
D.3.	Narodowy Instytut Standaryzacji i Technologii (NIST)	583
Dodatek E	Podstawowe koncepcje algebry liniowej	585
E.1.	Operacje na wektorach i macierzach	586
E.2.	Operacje algebry liniowej w arytmetyce zbioru Z_n	590
Dodatek F	Miara poufności i bezpieczeństwa kryptosystemów	591
F.1.	Poufność doskonała	592
F.2.	Informacja i entropia	597
F.3.	Entropia a poufność	603
Dodatek G	Uproszczony szyfr DES (SDDES)	605
G.1.	Ogólny schemat	606
G.2.	Generowanie kluczy	608
G.3.	Szyfrowanie	609
G.4.	Analiza S-DES	612
G.5.	Związek z DES	613
Dodatek H	Kryteria ewaluacyjne dla standardu AES	615
H.1.	Geneza standardu AES	616
H.2.	Ewaluacja AES	617
Dodatek I	Trochę więcej na temat uproszczonego AES	623
I.1.	Arytmetyka w ciele $GF(2^4)$	624
I.2.	Funkcja MixColumns	624

Dodatek J	Algorytm plecakowy kryptografii z kluczami publicznymi	627
J.1.	Problem plecakowy	628
J.2.	Kryptosystem plecakowy	628
J.3.	Przykład	632
Dodatek K	Dowód poprawności algorytmu DSA	635
Dodatek L	Protokół TCP/IP i architektura OSI	637
L.1.	Protokoły i architektury protokołów	638
L.2.	Architektura protokołu TCP/IP	640
L.3.	Rola protokołu IP	647
L.4.	Protokół IP w wersji 4 (IPv4)	650
L.5.	Protokół IP w wersji 6 (IPv6)	651
L.6.	Architektura protokołów OSI	656
Dodatek M	Biblioteki kryptograficzne języka Java	659
M.1.	Architektura JCA i JCE	660
M.2.	Klasy JCA	662
M.3.	Klasy JCE	664
M.4.	Podsumowanie	665
M.5.	Publikacje cytowane	665
Dodatek M.A	Przykładowa aplikacja kryptograficzna	666
Dodatek M.B	Kod źródłowy aplikacji — ilustracja zastosowania JCA/JCE	670
Dodatek N	Whirlpool	701
N.1.	Struktura funkcji Whirlpool	703
N.2.	Szyfr blokowy W	706
	Literatura cytowana	713
Dodatek O	Algorytm ZIP	715
O.1.	Algorytm kompresji	717
O.2.	Algorytm dekompresji	718
Dodatek P	Generowanie liczb losowych w PGP	721
P.1.	Generowanie liczb prawdziwie losowych	722
P.2.	Generowanie liczb pseudolosowych	722
Dodatek Q	Międzynarodowy alfabet wzorcowy (IRA)	725
Słownik		731
Bibliografia		741
Skorowidz		749