Spis treści

1 Podstawowe pojęcia i historia kryptografii 1
1.1 Wstęp do kryptografii 1
1.1.1 Szyfrowanie 1
1.1.2 Algorytmy i klucze 2
1.1.3 Zasady konstruowania mocnych systemów kryptograficznych 4
1.1.4 Złożoność obliczeniowa algorytmów 5
1.2 Proste szyfry strumieniowe 10
1.2.1 Szyfr Cezara 10
1.2.2 Szyfrowanie przy pomocy funkcji XOR (kod Vernama) 11
1.3 Proste szyfry blokowe 12
1.3.1 Permutacje 12
1.3.2 Transpozycje 12
1.3.3 Przykład blokowego szyfru przestawieniowego 13
1.3.4 Przykład blokowego szyfru podstawieniowego 16
1.3.5 Przykład szyfru produktowego 17
1.3.6 Uogólnienia podstawień - bigramy 18
1.3.7 Podstawienia polialfabetyczne 19
1.3.8 Szyfr Vigenera 20
1.4 Cylindry szyfrujące i maszyny wirnikowe 20
1.4.1 Cylindry szyfrujące 20
1.4.2 Maszyny wirnikowe 21
1.4.3 Enigma 22

2 Matematyczne podstawy krypfografii 25
2.1 Elementy teorii struktur algebraicznych 25
2.1.1 Grupy 26
2.1.2 Pierścienie i ciała 27
2.1.3 Ciała skończone 31
2.1.4 Pierścień wielomianów 32
2.1.5 Zastosowania ciał Galois 36

2.2 Elementy teorii liczb . . . 37
2.2.1 Podzielność . . . 37
2.2.2 Liczby pierwsze i ich własności . . . 39
2.2.3 Funkcja Eulera . . . 42
2.2.4 Kongruencje . . . 43
2.2.5 Równania proste . . . 44
2.2.6 Twierdzenie Eulera . . . 45
2.3 Sito Eratostenesa, algorytmy Euklidesa . . . 46
2.3.1 Sito Eratostenesa . . . 46
2.3.2 Algorytm Euklidesa . . . 47
2.3.3 Rozszerzony algorytm Euklidesa . . . 50
2.4 Algorytmy testowania pierwszości . . . 53
2.4.1 Test Fermata . . . 53
2.4.2 Test pierwszości Fermata . . . 54
2.4.3 Test Millera-Rabina . . . 55
2.4.4 Algorytm AKS . . . 56
2.5 Trudne obliczeniowo problemy teorii liczb . . . 56
2.5.1 Faktoryzacja . . . 56
2.5.2 Problem logarytmu dyskretnego . . . 59

3 Podstawy kryptografii symetrycznej . . . 61
3.1 Idea kryptografii symetrycznej . . . 61
3.1.1 Sieci Feistela . . . 62
3.2 Algorytm DES . . . 63
3.2.1 Szyfrowanie przy pomocy S-boxów . . . 63
3.2.2 Opis algorytmu DES . . . 64
3.3 Rozszerzenia algorytmu DES . . . 68
3.3.1 Trzykrotny DES . . . 68
3.3.2 DESX . . . 69
3.4 Tryby pracy algorytmu DES . . . 69
3.4.1 Tryb elektronicznej książki kodowej . . . 69
3.4.2 Tryb wiązania bloków zaszyfrowanych . . . 70
3.4.3 Tryb szyfrowania ze sprzężeniem zwrotnym . . . 70
3.5 Algorytm IDEA . . . 72
3.6 Algorytm RC5 . . . 74
3.6.1 Konkurs łamania RC5 . . . 75
3.7 Algorytm AES . . . 77
3.7.1 AES - następca algorytmu DES . . . 78
3.7.2 Podstawy matematyczne algorytmu AES . . . 78
3.7.3 Opis algorytmu . . . 86
3.7.4 Rozszerzenie klucza . . . 88
3.7.5 Algorytm szyfrowania . . . 90
3.7.6 Algorytm deszyfrowania . . . 91

3.8 Uogólnienia i wzmocnienia algorytmów DES, IDEA i AES 93
3.8.1 Algorytmy DES−768, IDEA−832 oraz AES−1408, AES−1664 i AES−1920 94
3.8.2 Uogólnione szyfry DES i AES 94

4 Podstawy kryptografii asymetrycznej 97
4.1 Idea kryptografii asymetrycznej 97
4.2 Algorytm Diffie-Hellmanna 98
4.3 Algorytm ElGamala 99
4.4 Algorytm RSA 100
4.4.1 Generowanie kluczy RSA 100
4.4.2 Szyfrowanie i deszyfrowanie 101

5 Podpis elektroniczny 105
5.1 Algorytmy podpisu cyfrowego, podpis elektroniczny 105
5.1.1 Podpis cyfrowy 106
5.1.2 Podpis realizowany przy pomocy RSA 107
5.1.3 Podpis ElGamala 108
5.1.4 Podpis realizowany przy pomocy DSA 109
5.2 Funkcje skrótu 110
5.2.1 Klasyfikacja funkcji skrótu 111
5.2.2 Funkcje skrótu z rodziny MD 112
5.2.3 Funkcje skrótu z rodziny SHA 116

6 System PGP 119
6.1 Historia, instalacja i wstępna konfiguracja PGP 119
6.1.1 Idea i historia PGP 119
6.1.2 Algorytmy PGP 121
6.1.3 Instalacja oprogramowania 124
6.1.4 Konfiguracja wstępna 125
6.1.5 Eksport, import i właściwości kluczy 127
6.1.6 Szyfrowanie i deszyfrowanie dokumentów 131
6.1.7 Podpis elektroniczny i weryfikacja podpisu w PGP 133
6.1.8 Struktura zaufania i certyfikowanie kluczy 133
6.2 PGPDesktop Professional 134
6.3 FireGPG 135

7 Infrastruktura klucza publicznego 137
7.1 Pojęcie infrastruktury klucza publicznego i jej podstawowe usługi 137
7.2 Współczesne zagrożenia w sieci 138
7.3 Zaufana trzecia strona, certyfikacja 138
7.4 PKI 142
7.5 Certyfikaty, klucze i zarządzanie nimi 145
7.5.1 Generowanie oraz instalacja certyfikatów 145

7.5.2 Konfiguracja certyfikatów . . . 147
7.5.3 Unieważnianie certyfikatów . . . 153

8 Protokoły kryptograficzne . . . 155
8.1 Przykłady protokołów kryptograficznych . . . 156
8.2 Wiarygodność . . . 157
8.2.1 Protokół Needhama-Schroedera . . . 158
8.3 Protokół Needhama-Schroedera z Centrum Certyfikacji . . . 161
8.4 Znaczniki czasu . . . 162
8.5 Protokół wymiany klucza z kluczem publicznym . . . 163
8.6 System Kerberos . . . 164
8.6.1 Opis protokołów składowych systemu Kerberos . . . 165
8.6.2 Przyklad wykorzystania systemu Kerberos . . . 167
8.7 Weryfikacja poprawności protokołów kryptograficznych . . . 168
8.7.1 Metoda aksjomatyczna (dedukcyjna) . . . 169
8.7.2 Weryfikacja modelowa (ang. model checking) . . . 170
8.7.3 Metoda indukcyjna . . . 170
8.7.4 Wyniki . . . 171
8.7.5 Podsumowanie . . . 172

9 Zastosowania kryptografii do ochrony danych . . . 173
9.1 Poufność poczty elektronicznej . . . 173
9.1.1 PEM . . . 174
9.1.2 PGP . . . 175
9.1.3 S/MIME . . . 176
9.1.4 MOSS . . . 178
9.1.5 GNUPGP . . . 178
9.2 Zabezpieczenia wymiany dokumentów . . . 178
9.2.1 EDI . . . 179
9.2.2 OpenEDI . . . 180
9.2.3 OBI . . . 180
9.2.4 Swift, Edifact . . . 180
9.2.5 EDI w praktyce . . . 181
9.2.6 Elixir . . . 182
9.3 Bezpieczeństwo w sieci SSH i SSL . . . 182
9.3.1 Wstęp . . . 183
9.3.2 Idea protokołu SSH . . . 184
9.3.3 Zastosowanie protokołu SSH . . . 186
9.3.4 Budowa protokołu SSL . . . 187
9.3.5 Zastosowanie SSL w praktyce . . . 190

Literatura . . . 193