

Spis treści

O autorze 11

Podziękowania 13

Wprowadzenie 15

Rozdział 1. Wprowadzenie do kryptografii i Pythona 19

Algorytmy 19

Dlaczego warto korzystać z Pythona? 20

Pobieranie i instalacja Pythona 21

Instalacja na Ubuntu 21

Instalacja w systemie macOS 22

Instalacja w systemie Windows 22

Instalacja na chromebooku 23

Instalowanie dodatkowych pakietów 23

Instalacja Pip, NumPy, Matplotlib i SciPy 23

Instalacja pakietu Cryptography 25

Instalacja dodatkowych pakietów 25

Testowanie instalacji 26

Podstawy Pythona 26

Zmienne 27

łańcuchy znaków 27

Operatory 28

Operatory arytmetyczne 28

Operatory porównania 29

Operatory logiczne 30

Operatory przypisania 30

Operatory bitowe 30

Operatory przynależności 31

Operatory tożsamości 32

Wyrażenia warunkowe 32

Pętle 33

for 33

while 33

continue 34

break 34

else 34

Praca z plikami 34

Semantyka Pythona 35

Typy sekwencyjne 36

Własne funkcje 41

Pobieranie plików 42

Moduły 43

Szyfr wsteczny 44

Podsumowanie 44

Rozdział 2. Protokoły kryptograficzne i poufność doskonała 45

Studium kryptologii 46

Zrozumieć kryptografię 46

Alicja i Bob, czyli słynna kryptograficzna rodzina 47

Protokół Diffiego-Hellmana 48

Uwierzytelnianie źródła danych 48

Uwierzytelnianie jednostek 49

Algorytmy symetryczne 50

Algorytmy asymetryczne 50

Protokoły Needhama-Schroedera 50

Protokół Otway-Reesa 52

Kerberos 52

Kerberos w wielu domenach 54

X.509 55

Konfiguracja Twojej pierwszej biblioteki kryptograficznej 56

Formalna walidacja protokołów kryptograficznych 59

Zrozumieć kryptoanalizę 60

Modele ataków 60

Ataki metodą siłową 61

Ataki kanałem bocznym 61

Inżynieria społeczna 62

Ataki analityczne 62

Analiza częstości 62

Twierdzenie Shannona 62

Szyfr z kluczem jednorazowym 63

XOR, AND i OR 63

Funkcja szyfru z kluczem jednorazowym 67

Jednokierunkowe funkcje skrótu 70

Jednokierunkowe kryptograficzne funkcje skrótu 70

Kody uwierzytelniania wiadomości 71

Doskonałe utajnianie z wyprzedzaniem 72

Opublikowane i zastrzeżone algorytmy szyfrowania 73

Podsumowanie 73

Bibliografia 74

Rozdział 3. Kryptografia klasyczna 75

Najlepsze praktyki dotyczące haseł 75

Przechowywanie haseł 76

Haszowanie haseł 76

Solenie haseł 77

Password/keystretching 78

Narzędzia przydatne w pracy z hasłami 78

Zaciemnianie danych 79

Kodowanie ASCII 79

Kodowanie tekstu Base64 79

Dane binarne 81

Dekodowanie 81

Szyfry o znaczeniu historycznym 82

Spartańskie Skytale 82

Szyfry podstawieniowe 82

Szyfr Cezara 83

ROT-13 84

Atbasz 85

Szyfr Vigenere'a 86

Szyfr Playfaira 87

Szyfr Hilla 2×2 90

Kolumnowy szyfr przestawieniowy 94

Szyfr afiniczny 97

Podsumowanie 99

Rozdział 4. Matematyka kryptograficzna i analiza częstości 101

Arytmetyka modularna i największy wspólny dzielnik 102

Liczby pierwsze 103

Twierdzenie o liczbach pierwszych 104

Szkolny test pierwszości 104

Małe twierdzenie Fermata 105

Test pierwszości Millera-Rabina 106

Generowanie dużych liczb pierwszych 109

Podstawy teorii grup 111

Rząd elementu 112

Odwrotność modulo 114

Odwrotność z użyciem małego twierdzenia Fermata 114

Rozszerzony algorytm Euklidesa 115

Twierdzenie Eulera 115

Pseudolosowość 118

Funkcja generująca wartości pseudolosowe	119
Rozwiązywanie układów równań liniowych	120
Analiza częstości	123
Kryptoanaliza z użyciem Pythona	126
Korzystanie z internetowej listy słów	128
Obliczanie częstości znaków	128
Łamanie szyfru Vigenere'a	131
Podsumowanie	138

Rozdział 5. Szyfry strumieniowe i blokowe 139

Konwersja pomiędzy zapisem szesnastkowym a tekstem jawnym	140
Szyfry strumieniowe	141
ARC4	146
Szyfr Vernama	147
Szyfr Salsa20	148
Szyfr ChaCha	150
Szyfry blokowe	154
Tryb ECB	156
Tryb CBC	157
Tryb CFB	158
Tryb OFB	159
Tryb CTR	160
Tryby strumieniowe	162
Samodzielne tworzenie szyfru blokowego za pomocą sieci Feistela	162
Advanced Encryption Standard (AES)	164
AES w Pythonie	164
Szyfrowanie plików za pomocą AES	166
Odszyfrowywanie plików za pomocą AES	166
Podsumowanie	166

Rozdział 6. Kryptografia wizualna 167

Prosty przykład 167

Biblioteki graficzne i steganograficzne 169

 Biblioteka cryptography 170

 Biblioteka cryptosteganography 170

Kryptografia wizualna 171

 Szyfrowanie zawartości pliku za pomocą algorytmu Fernet 171

 Szyfrowanie obrazu za pomocą algorytmu Fernet 173

 AES i tryby kodowania 174

 Prosty przykład użycia trybu ECB 175

 Prosty przykład szyfrowania w trybie CBC 179

 Wykorzystanie wiedzy w praktyce 180

Steganografia 181

 Przechowywanie wiadomości w obrazie 181

 Ukrywanie pliku binarnego w obrazie 184

 Praca z dużymi obrazami 187

Podsumowanie 189

Rozdział 7. Integralność wiadomości 191

 Kody uwierzytelniania wiadomości 191

 Kod uwierzytelniania wiadomości oparty na funkcjach haszujących 193

 Podpisywanie wiadomości za pomocą HMAC 194

 Podpisywanie algorytmem SHA 194

 Skróty binarne 195

 Zgodność z NIST 197

 CBC-MAC 198

 Atak urodzinowy 199

 Fałszowanie wiadomości 200

 Atak length extension 200

Ustanawianie bezpiecznego kanału komunikacji 201

 Kanały komunikacyjne 202

 Przesyłanie bezpiecznych wiadomości przez sieci IP 202

Tworzenie gniazda serwera	203
Tworzenie gniazda klienta	204
Tworzenie wielowątkowego serwera z komunikacją TCP	204
Dodawanie szyfrowania symetrycznego	205
Łączenie wiadomości i kodu MAC	208
Podsumowanie	211
Bibliografia	211
 Rozdział 8. Infrastruktura klucza publicznego i zastosowania kryptografii	213
Koncepcja klucza publicznego	214
Podstawy RSA	216
Generowanie certyfikatu RSA	218
Szyfrowanie i odszyfrowywanie tekstu za pomocą certyfikatów RSA	220
Szyfrowanie i odszyfrowywanie obiektów BLOB za pomocą certyfikatów RSA	221
Algorytm ElGamal	223
Kryptografia krzywych eliptycznych	226
Generowanie kluczy w ECC	228
Długości klucza i krzywe	229
Protokół wymiany kluczy Diffiego-Hellmana	230
Podsumowanie	232
 Rozdział 9. Szlifowanie umiejętności kryptograficznych w Pythonie	233
Tworzenie aplikacji do niezaszyfrowanej komunikacji	234
Tworzenie serwera	234
Tworzenie klienta	236
Tworzenie pliku pomocniczego	237
Uruchamianie	238
Instalowanie i testowanie Wiresharka	238
Implementacja PKI z użyciem certyfikatów RSA	240
Modyfikowanie serwera	241
Modyfikowanie klienta	242

Modyfikowanie pliku pomocniczego 243

Uruchamianie 244

Implementacja protokołu wymiany kluczy Diffiego-Hellmana 245

Modyfikowanie kodu serwera 247

Modyfikowanie kodu klienta 248

Modyfikowanie pliku pomocniczego 250

Klasa DiffieHellman 254

Uruchamianie 258

Podsumowanie 259