

spis treści

przedmowa xv

podziękowania xix o

książce xxi

o autorze xxvii

CZĘŚĆ I PRYMITYWY. SKŁADNIKI KRYPTOGRAFII 1

1 Wprowadzenie 3

1.1. W kryptografii chodzi o zabezpieczenie protokołów 4

1.2. Kryptografia symetryczna. Czym jest szyfrowanie symetryczne? 5

1.3. Zasada Kerckhoffs'a: tylko klucz pozostaje tajny 7

1.4. Kryptografia asymetryczna. Dwa klucze są lepsze niż jeden 10

O wymianianiu się kluczami albo jak uzyskać dostęp do wspólnego sekretu 11 ■
Szyfrowanie asymetryczne, nie mylić z symetrycznym 14 ■ Podpisy cyfrowe, zupełnie
jak te tradycyjne 16

1.5. Kryptografia: klasyfikacje i abstrakcje 18

1.6. Kryptografia teoretyczna a prawdziwy świat kryptografii 20

1.7. Od teorii do praktyki. Każdy może pójść własną ścieżką 21

1.8. Słowo ostrzeżenia 26

2	Funkcje skrótu (funkcje haszujące)	28
2.1.	Czym jest funkcja skrótu?	29
2.2.	Właściwości zabezpieczeń funkcji skrótu	32
2.3.	Uwarunkowania zabezpieczeń funkcji skrótu	34
2.4.	Funkcje skrótu w praktyce	36
	Zobowiązania 36 ■ Integralność zasobów podrzędnych 36 ■ BitTor-rent 37 ■ Tor 37	
2.5.	Znormalizowane funkcje skrótu	38
	Funkcja haszująca SHA-2 39 ■ Funkcja haszująca SHA-3 43 ■ SHAKE i cSHAKE. Dwie funkcje o rozszerzalnym wyjściu (XOF) 47 ■ Jak uniknąć wieloznacznego haszowania za pomocą TupleHash 48	
2.6.	Haszowanie haseł	50
3	Kody uwierzytelniania wiadomości	54
3.1.	Ciasteczka bezstanowe - motywujący przykład dla MAC	55
3.2.	Kod z przykładem	58
3.3.	Właściwości zabezpieczeń MAC	59
	Falszerstwo znacznika uwierzytelniania 59 ■ Długość znacznika uwierzytelniania 60 ■ Ataki powtórzeniowe 60 ■ Weryfikacja znaczników uwierzytelniania w stałym czasie 62	
3.4.	MAC w prawdziwym świecie	64
	Uwierzytelnianie wiadomości 64 ■ Wyprowadzanie kluczy 64 ■ Integralność ciasteczek 65 ■ Tablice mieszające 65	
3.5.	Kody uwierzytelniania wiadomości w praktyce	65
	HMAC, czyli MAC oparty na haszu 65 ■ KMAC, czyli MAC oparty na cSHAKE 67	
3.6.	SHA-2 i ataki przedłużenia długości	67
4	Szyfrowanie uwierzytelnione	71
4.1.	Czym jest szyfr?	72
4.2.	Szyfr blokowy AES	74
	Jaki poziom bezpieczeństwa zapewnia AES? 74 ■ Interfejs AES 75 ■ Wewnętrzna konstrukcja AES 76	
4.3.	Zaszyfrowany pingwin i tryb CBC	78
4.4.	Na brak uwierzytelnienia - AES-CBC-HMAC	81
4.5.	Konstrukcje typu „wszystko w jednym”. Szyfrowanie uwierzytelnione	83
	Czym jest szyfrowanie uwierzytelnione z powiązаныmi danymi (AEAD)? 83 ■ Algorytm AEAD o nazwie AES-GCM 85 ■ ChaCha20-Poly1305 90	
4.6.	Inne rodzaje szyfrowania symetrycznego	94
	Opakowywanie klucza 94 ^ Szyfrowanie uwierzytelnione odporne na niepoprawne użycie nonce 95 ^ Szyfrowanie dysku 95 ^ Szyfrowanie baz danych 96	

5	Wymiany klucza	98
5.1.	Czym są wymiany klucza?	99
5.2.	Wymiana klucza Diffiego-Hellmana (DH)	102
	Teoria grup 102 ^ Problem logarytmu dyskretnego. Fundament algorytmu Diffiego-Hellmana 107 ^ Normy algorytmu Diffiego-Hellmana	109
5.3.	Wymiana kluczy przy użyciu protokołu Diffiego-Hellmana w przestrzeni krzywych eliptycznych	110
	Czym jest krzywa eliptyczna? 111 ^ Jak działa algorytm Diffiego-Hellmana oparty na krzywych eliptycznych? 114 ^ Normy dla algorytmu Diffiego-Hellmana w przestrzeni krzywych eliptycznych	116
5.4.	Atak przeciwko małym podgrupom i inne czynniki związane z bezpieczeństwem	118
6	Szyfrowanie asymetryczne i szyfrowanie hybrydowe	123
6.1.	Czym jest szyfrowanie asymetryczne?	124
6.2.	Szyfrowanie asymetryczne i szyfrowanie hybrydowe w praktyce	126
	Wymiany klucza i kapsułkowanie klucza 127 ^ Szyfrowanie hybrydowe	128
6.3.	Szyfrowanie asymetryczne przy użyciu RSA: złe i mniej złe	132
	Podręcznikowe RSA 132 ^ Dlaczego nie należy używać RSA PKCS#1 v1.5 137 ■ Szyfrowanie asymetryczne przy użyciu RSA-OAEP	139
6.4.	Szyfrowanie hybrydowe przy użyciu ECIES	142
7	Podpisy i dowody z wiedzą zerową	145
7.1.	Czym jest podpis?	146
	Jak w praktyce weryfikować podpisy 147 ^ Najważniejszy przypadek użycia podpisów, czyli uwierzytelnione wymiany klucza 148 ^ Rzeczywisty przypadek użycia. Infrastruktura klucza publicznego	149
7.2.	Dowody z wiedzą zerową (ZKP). Pochodzenie podpisów	151
	Protokół identyfikacji Schnorra. Interaktywny dowód z wiedzą zerową 151 ■ Podpisy jako nieinteraktywne dowody z wiedzą zerową	154
7.3.	Algorytmy podpisów, z których powinniśmy korzystać (lub nie)	156
	RSA PKCS#1 v1.5, czyli zła norma 157 ■ RSA-PSS. Lepsza norma 160 ^ Algorytm podpisu elektronicznego oparty na krzywych eliptycznych 161 ■ Algorytm podpisu cyfrowego oparty na krzywej Edwardsa	164
7.4.	Subtelności schematów podpisów	168
	Ataki podstawieniowe na podpisy 168 ^ Deformowalność podpisu	169
8	Losowość i sekrety	172
8.1.	Czym jest losowość?	173
8.2.	Powolna losowość? Skorzystajmy z generatora liczb pseudolosowych (PRNG)	175
8.3.	Uzyskiwanie losowości w praktyce	179
8.4.	Generowanie losowości i czynniki związane z bezpieczeństwem	181

8.5. Publiczna losowość	184
8.6. Wyprowadzanie kluczy za pomocą HKDF	186
8.7. Zarządzanie kluczami i sekretami	190
8.8. Decentralizacja zaufania za pomocą kryptografii progowej	192
CZĘŚĆ II PROTOKOŁY, CZYLI PRZEPISY NA KRYPTOGRAFIĘ	197
9 Bezpieczny transport	199
9.1. Bezpieczne protokoły transportowe: SSL i TLS	199 Od
SSL do TLS	200 ■ TLS w praktyce
201	
9.2. Jak działa protokół TLS?	203
Handshake TLS	204 ■ Jak TLS 1.3 szyfruje dane aplikacji
218	
9.3. Aktualny stan szyfrowania w sieci web	219
9.4. Inne bezpieczne protokoły transportowe	222
9.5. Framework protokołu Noise. Współczesna alternatywa dla TLS	222 Wiele
odcieni fazy handshake	223 ^ Handshake przy użyciu Noise
224	
10 Szyfrowanie od końca do końca	227
10.1. Dlaczego szyfrowanie od końca do końca?	228
10.2. Niemożliwe do odnalezienia źródło zaufania	230
10.3. Porażka szyfrowanych e-maili	231
PGP czy GPG? I jak to w ogóle działa?	232 ■ Skalowanie zaufania pomiędzy
użytkownikami za pomocą sieci zaufania	235 ■ Odkrywanie kluczy to prawdziwy
problem	236 ■ Jeśli nie PGP, to co?
238	
10.4. Bezpieczne przesyłanie wiadomości. Nowoczesne spojrzenie	
na szyfrowanie od końca do końca w aplikacji Signal	239
Bardziej przyjazny dla użytkownika niż WOT. Ufaj, ale weryfikuj	241 ■ X3DH.
Handshake protokołu Signal	243 ■ Podwójna Zapadka. Protokół post-handshake
Signalu	247
10.5. Stan szyfrowania od końca do końca	252
11 Uwierzytelnianie użytkownika	256
11.1. Uwierzytelnianie - kilka słów podsumowania	257
11.2. Uwierzytelnianie użytkownika, czyli jak pozbyć się haseł	259
Jedno hasło, by rządzić wszystkimi. Pojedyncze logowanie (SSO) i menedżery haseł	261 ■ Nie chcecie widzieć haseł? Użyjcie asymetrycznej wymiany kluczy
uwierzytelnianej hasłem	263 ■ Hasła jednorazowe to tak naprawdę nie hasła.
Bezhasłowość przy użyciu kluczy symetrycznych	268 ■ Jak zastąpić hasła kluczami
asymetrycznymi	271
11.3. Uwierzytelnianie wspomagane przez użytkownika - parowanie urządzeń	
wykorzystujące wsparcie człowieka	274

Klucze wstępnie współdzielone 276 ■ Symetryczne uwierzytelnianie hasłem wymiany klucza przy użyciu CPace 278 ■ Czy naszą wymianę klucza zaatakował pośrednik? Po prostu sprawdźmy krótki ciąg uwierzytelniony (SAS) 279

12 Krypto jak w słowie „kryptowaluta”? 285

12.1. Wprowadzenie do algorytmów konsensusu tolerancyjnych na bizantyjskie błędy 286

Problem odporności. Protokoły rozproszone przychodzą na ratunek 287 ■ Problem zaufania? Decentralizacja przychodzi z pomocą 288 ■ Problem skali. Sieci bezpozwoleniowe i odporne na cenzurę 290

12.2. Jak działa bitcoin? 292

W jaki sposób bitcoin obsługuje salda użytkownika i transakcje 292 ■ Wydobywanie bitcoinów w cyfrowej złotej erze 294 ■ Jasny fork! Rozwiązywanie konfliktów wydobywczych 298 ■ Redukcja rozmiaru bloku za pomocą drzew Merkle 301

12.3. Wycieczka po świecie kryptowalut 303

Zmienna wartość 303 ^ Latencja 303 ^ Rozmiar łańcucha bloków 304
 ■ Poufność 304 ■ Wydajność energetyczna 304

12.4. DiemBFT. Tolerancyjny na bizantyjskie błędy protokół konsensusu 305

Bezpieczeństwo i żywotność. Dwie własności protokołu konsensusu BFT 305 ^ Runda w protokole DiemBFT 306 ^ Ile nieuczciwości może tolerować protokół? 307 ^ Zasady głosowania DiemBFT 308 ^ Kiedy transakcje uważa się za sfinalizowane? 309 ^ Intuicje stojące za bezpieczeństwem DiemBFT 310

13 Kryptografia sprzętowa 314

13.1. Model napastnika we współczesnej kryptografii 315

13.2. Niezaufane środowiska. Sprzęcie, ratuj! 316

Kryptografia białej skrzynki - zły pomysł 317 ^ Siedzą w naszych portfelach. Inteligentne karty i bezpieczne elementy 318 ^ Banki je uwielbiają. Sprzętowe moduły bezpieczeństwa 320 ^ Moduły zaufanej platformy (TPM). Przydatna normalizacja elementów bezpiecznych 323 ■ Poufne obliczenia z zaufanym środowiskiem wykonawczym 327

13.3. Które rozwiązanie będzie dobre dla mnie? 328

13.4. Kryptografia odporna na wycieki, czyli jak złagodzić ataki kanałem bocznym w oprogramowaniu 330

Programowanie stałoczasowe 332 ^ Nie korzystaj z sekretu! Maskowanie 334
 ■ A co z atakami usterek? 335

14 Kryptografia postkwantowa 338

14.1. Czym są komputery kwantowe i dlaczego straszą kryptografów? 339

Mechanika kwantowa - studium rzeczy małych 340 ^ Od narodzin komputerów kwantowych po supremację kwantową 342 ^ Wpływ algorytmów Grovera i Shora na kryptografię 343 ^ Kryptografia postkwantowa, czyli jak się bronić przed komputerami kwantowymi 345

14.2. Podpisy oparte na haszach. Nie potrzeba niczego poza funkcją skrótu 346

Podpisy jednorazowe (OTS) z podpisami Lamporta 346 ^ Mniejsze klucze i jednorazowe podpisy Winternitza 348 ^ Podpisy wielorazowe z XMSS oraz SPHINCS+ 349

14.3. Krótsze klucze i podpisy dzięki kryptografii opartej na kratkach	353
Czym jest krata? 353 ^ Uczenie się z błędami podstawą kryptografii? 355 ^ Kyber, czyli wymiana klucza oparta na kracie 356 ■ Dilithium - schemat podpisu oparty na kracie	359
14.4. Czy powinniśmy zacząć panikować?	360
15 Czy to już wszystko? Kryptografia następnej generacji	364
15.1. Im więcej, tym lepiej. Bezpieczne obliczenia wielostronne	365
Przecięcie zbiorów prywatnych (PSI) 366 ^ MPC ogólnego przeznaczenia 367 ■ Stan MPC	370
15.2. W pełni homomorficzne szyfrowania i obietnica zaszyfrowanej chmury	370
Przykład szyfrowania homomorficznego z szyfrowaniem RSA 371 ^ Różne typy szyfrowania homomorficznego 371 ^ Bootstrapping, klucz do w pełni homomorficznego szyfrowania 372 ^ Schemat FHE oparty na problemie uczenia się z błędami 374 ^ Gdzie się z tego korzysta? 376	
15.3. Dowody z wiedzą zerową ogólnego przeznaczenia	377
15.3.1. Jak działają schematy zk-SNARK 380 ^ Zobowiązania homomorficzne - ukrywamy części dowodu 381 ^ Parowania bilinearne - ulepszymy nasze zobowiązania homomorficzne 381 ^ Skąd się bierze zwięzłość? 382 ^ Od programów do wielomianów 384 ^ Programy są dla komputerów; nam potrzebne są układy arytmetyczne 383 ■ Układy arytmetyczne R1CS 384 ■ Od R1CS do wielomianu 385 ^ Trzeba dwojga, aby określić wartość wielomianu ukrytego w wykładniku	386
16 Kiedy i gdzie kryptografia zawodzi	389
16.1. Szukanie właściwego prymitywu kryptograficznego lub protokołu to nudna praca	390
16.2. W jaki sposób korzystam z prymitywu kryptograficznego lub protokołu? Uprzejme normy i formalna weryfikacja	392
16.3. Gdzie są dobre biblioteki?	395
16.4. Niewłaściwe wykorzystanie kryptografii. Programiści to wrogowie	396
16.5. Robicie to źle. Użyteczne zabezpieczenia	397
16.6. Kryptografia nie jest wyspą	399
16.7. Nasze obowiązki jako praktyków kryptografii. Dlaczego nie powinniśmy wdrażać własnej kryptografii	400
Dodatek Odpowiedzi do ćwiczeń	404
Rozdział 2	404
Rozdział 3	405
Rozdział 6	405
Rozdział 7	406
Rozdział 8	406
Rozdział 9	406

Rozdział 10 407

Rozdział 11 407