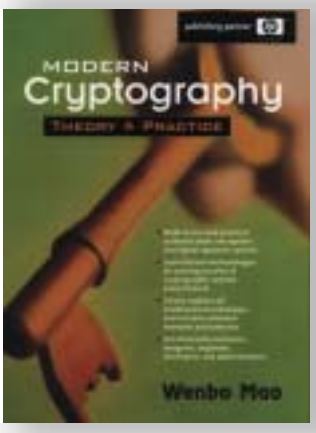
Modern Cryptography
Theory & Practice
Wenbo Mao



Kryptografie jako obor prochází v posledním desetiletí bouřlivým vývojem, nové publikace, které jsou nyní vydávány jsou toho velice dobrým dokladem. Nejznámější knihu v této kategorii - Applied Cryptography napsal v roce 1994 Bruce Schneier. Obdobně byla úspěšná kniha autorů A.J.Menezes, P. C. van Oorschot a S.A.Vanstone: Handbook of Applied Cryptography[1], 1996. Tyto knihy svým encyklopedickým charakterem se staly na dlouhou dobu základními příručkami v oboru. Od vydání obou knih však již uplynul nějaký čas, byla získána celá řada nových výsledků. Celý obor se také posunul od víceméně matematického popisu algoritmů k řešení rozsáhlé řady dalších otázek souvisejících především s praktickým zaváděním kryptografických technik. Objevila se například celá řada nových útoků na konkrétní kryptografické protokoly, význačným posunem bylo také například zvažování tzv. postranních kanálů, některé aplikace vyžadují jiné formální přístupy k hodnocení bezpečnosti atd.

Recenzovaná kniha se svým rozsahem (cca 700 stran) i zaměřením na kryptografické aplikace stává vysoce užitečnou příručkou nového typu. Autor nic neslevil na teoretické úrovni, používá rigorózní matematický aparát. Některé momenty (jako například vazby na teorii výpočetní složitosti, základy teorie čísel) jsou zde uvedeny na úrovni nezbytné pro chápání všech kryptografických souvislostí. Směruje však knihu nikoliv k obvyklému popisu kryptografie v ideálním světě (což je cesta, kterou jde řada autorů knih učebnicového typu), ale jeho cílem je přenést teorii do reálného světa, tedy posoudit nejen teoretickou bezpečnost použitých postupů, ale i bezpečnostní vlastnosti konkrétních aplikací. Z hlediska tohoto pohledu je jedině žádoucí knihu doporučit jak odborníkům tak i jako učebnici pro novou generaci kryptografů.

Kniha sestává z šesti částí (a 20 kapitol). První - úvodní - část je úvodem do problematiky kryptografie a informační bezpečnosti. Autor vysvětluje na jednoduchém kryptografickém protokolu základní filosofii problematiky. Ukazuje zde smysl zavádění kryptografických pojmů pro řešení praktických otázek bezpečnosti aplikací. Autor ukazuje, proč volba vhodného kryptografického modelu musí být prováděna na základě celé řady různorodých kriterií.

Druhou část (kapitoly 3-6) tvoří popis nezbytného matematického aparátu (teorie pravděpodobnosti, teorie výpočetní složitosti, algebraické metody a teorie čísel). V následujících částech knihy autor demonstruje nezbytnost těchto přístupů pro moderní analýzy kryptografických protokolů. V třetí části je popsána řada v současnosti nejznámějších kryptografických algoritmů - symetrické (DES, AES) a asymetrické kryptografie (Diffie-Hellman, RSA, ElGamal). Krátká kapitola 9 je věnována problematice bezpečnosti jednotlivého bitu pro systémy s veřejným klíčem (důležitá bezpečnostní vlastnost těchto systémů). V kapitole 10 je uveden pojem hashovací funkce a problematika uchování neporušenosti (integrity) dat.

Čtvrtá část (Autentizace) popisuje základní autentizační techniky a vlastnosti celé řady známých (i z norem) autentizačních protokolů. Například kapitola 12 je věnována popisu a analýze takových protokolů jako jsou IKE, IPSec, SSH, Kerberos a samozřejmě není opomenut ani protokol SSL (resp. jeho novější varianta TLS). Pátá část pojednává důležitý aspekt posuzování bezpečnosti reálných implementací kryptografických technik - zavádí formalizované postupy pro pojetí tzv. silné bezpečnosti a ukazuje jak na základě tohoto pojetí ustavit (tj. reálně zdůvodnit) faktická funkční schémata. Kapitoly 15. a 16 jsou věnovány důležité problematice prokazatelné bezpečnosti (systémů s veřejným klíčem a digitálních podpisů). V poslední šesté části knihy se autor věnuje problematice protokolů s nulovou znalostí, která je aktuální zejména pro různé aplikace elektronického obchodování.

TITUL: MODERN CRYPTOGRAPHY.
THEORY & PRACTICE.
AUTOR: WENBO MAO,
VYDALO: PRENTICE HALL, 2003,
ISBN: 0-13-066943-1,
CENA: 54,99 USD.

[1] Celou knihu lze nalézt online na adrese *http://www.cacr.math.uwaterloo.ca/hac/*

prosím krátit
děkuji

Celkově - u knihy je třeba ocenit zejména moderní pojetí problematiky. Dle soudu recenzenta se zámysl autora orientovat se především na aplikační aspekty dnešní kryptografie vydařil. Zejména druhou polovinu knihy (části IV, V a VI) lze doporučit čtenářům, kteří se orientují na problematiku bezpečnosti praktických aplikací.

Jaroslav Pinkava
jaroslav.pinkava@pvt.cz

Celou knihu lze nalézt online na adrese http://www.cacr.math.uwaterloo.ca/hac/