

New Frontiers in Cryptography

Khaled Salah Mohamed

New Frontiers in Cryptography

Quantum, Blockchain, Lightweight, Chaotic
and DNA



Springer

Khaled Salah Mohamed
A Siemens Business
Fremont, CA, USA

ISBN 978-3-030-58995-0 ISBN 978-3-030-58996-7 (eBook)
<https://doi.org/10.1007/978-3-030-58996-7>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*Dedicated to the memory of my grandfather
and grandmother.*

Preface

Today, cryptography plays a vital role in every electronic and communication system. Everyday, many users generate and interchange large amount of information in various fields through internet, telephone conversations and e-commerce transactions. In modern system-on-chips (SoCs), cryptography plays an integral role in protecting the confidentiality and integrity of information. This book provides comprehensive coverage of various cryptography topics, while highlighting the most recent trends such as quantum, blockchain, lightweight, chaotic and DNA cryptography. Moreover, this book covers cryptography primitives and their usage and applications and focuses on the fundamental principles of modern cryptography such as stream ciphers, block ciphers, public key algorithms and digital signatures. The readers will build a solid foundation in cryptography and security. This book presents the fundamental mathematical concepts of cryptography. Moreover, this book presents hiding data techniques such as steganography and watermarking. Besides, it provides a comparative study of the different cryptographic methods that can be used efficiently to solve security problems. This book discusses modern cryptography and data hiding techniques. This includes:

- *Stream ciphers, block ciphers, public key algorithms and digital signatures.*
- *Quantum cryptography:* Quantum cryptography uses physics to develop a cryptosystem completely secure against being compromised without the knowledge of the sender or the receiver of the messages.
- *Blockchain cryptography:* Blockchain is a distributed database that allows direct transactions between two parties without the need for an authoritative mediator. Blockchain cryptography is a way to encapsulate transactions in the form of blocks where blocks are linked through the cryptographic hash, hence forming a chain of secured blocks.
- *Lightweight cryptography:* Lightweight cryptography works between the trade-offs of security, cost, and performance and is focused at devices and systems on edge.
- *Chaotic cryptography:* Many strong ciphers have been applied widely, such as DES, AES and RSA. But most of them cannot be directly used to encrypt

real-time embedded systems because their encryption speed is not fast enough and they are computationally intensive. So, chaotic cryptography is suitable for real-time embedded systems in terms of performance, area and power efficiency.

- *DNA cryptography*: DNA cryptography is a promising and rapid emerging field in data security. DNA cryptography may bring forward a new hope for unbreakable algorithms. DNA cryptology combines cryptology and modern biotechnology.
- *Steganography*: Steganography is the art of hiding the existence of a message between sender and intended recipient. It hides secret messages in various types of files such as text, images, audio and video.
- *Watermarking*: Watermarking is embedding some information within a digital media so that the digital media looks unchanged. This is useful for copy protection.

Fremont, CA, USA

Khaled Salah Mohamed

Contents

1	Introduction to Cyber Security	1
1.1	Security Terms	1
1.2	Security Threats/Attacks	2
1.3	Security Requirements/Services/Objectives/Goals	2
1.3.1	Confidentiality	3
1.3.2	Authentication	3
1.3.3	Integrity	4
1.3.4	Access Control/Authorization	4
1.3.5	Availability	4
1.3.6	Non-repudiation	4
1.4	Security Mechanisms/Tools/Defenses	5
1.5	Security Hierarchy/Levels	6
1.6	Mathematical Background	9
1.6.1	Modular Arithmetic	9
1.6.2	Greatest Common Divisor	9
1.7	Security Protocols	9
1.7.1	SSL	10
1.7.2	IPSec	10
1.8	Conclusions	11
	References	11
2	Cryptography Concepts: Confidentiality	13
2.1	Cryptography History	13
2.2	Symmetric Encryption	14
2.2.1	Historical Algorithms: Letter-Based Algorithms	14
2.2.2	Modern Algorithms: Bits-Based Algorithms	18
2.3	Asymmetric Encryption	25
2.3.1	RSA: Factorization Computational Problem	26
2.3.2	ECC: Discrete Logarithm Problem (DLP)	27
2.3.3	ElGamal Cryptosystem	28
2.3.4	Diffie–Hellman Algorithm: Key Exchange	28

2.3.5	EGC	29
2.4	Hybrid Encryption	29
2.5	Crypto-Analysis/Attacks	29
2.5.1	Exhaustive/Brute Force Attack	30
2.5.2	Statistical/Histogram Attack	30
2.5.3	Differential Attack	31
2.5.4	Known/Chosen Plaintext/Ciphertext Attack	31
2.6	Comparison Between Different Encryption Algorithms	33
2.7	Cryptography Applications	34
2.7.1	Secured Email	34
2.7.2	Secured Chat	35
2.7.3	Secured Wireless Communication System	35
2.7.4	Secured Mobile/Smartphone	36
2.8	Conclusions	37
	References.....	37
3	Cryptography Concepts: Integrity, Authentication, Availability, Access Control, and Non-repudiation	41
3.1	Integrity: Hashing Concept	41
3.1.1	SHA-3	42
3.1.2	HMAC-SHA256 (Hashed Message Authentication Code, Secure Hash Algorithm)	43
3.1.3	MD5 Algorithm	51
3.1.4	Blake	51
3.2	Integrity: Digital Signature	52
3.3	Authentication	52
3.3.1	HDCP	53
3.3.2	CAPTCHA Codes	54
3.4	Availability: Intrusion Detection	54
3.4.1	Artificial Immune System	54
3.5	Access Control	60
3.6	Non-repudiation: Trusted Third Party	61
3.7	Conclusions	61
	References.....	61
4	New Trends in Cryptography: Quantum, Blockchain, Lightweight, Chaotic, and DNA Cryptography	65
4.1	DNA Cryptography	65
4.1.1	Fundamentals of DNA Computing	66
4.1.2	DNA Cryptography Algorithm	66
4.2	Quantum Cryptography	67
4.2.1	Properties of Quantum Information.....	68
4.2.2	Quantum Algorithms	69
4.2.3	Quantum Cryptography Challenges.....	70
4.3	Chaotic Cryptography	71
4.3.1	Chaotic Theory.....	71

4.3.2	Chaotic Encryption System	72
4.3.3	Hardware Implementation of Chaotic Algorithm	74
4.3.4	Evaluation of the Proposed Algorithm.	75
4.4	Lightweight Cryptography.	77
4.4.1	PRESENT Algorithm.	77
4.4.2	SIT Algorithm	79
4.4.3	HIGHT Algorithm	80
4.4.4	KHUDRA Algorithm.	80
4.4.5	CAMELLIA Algorithm	80
4.4.6	Attribute-Based Encryption (ABE)	81
4.5	Blockchain Cryptography	81
4.5.1	Limitations of Blockchain Technology Can Be Summarized as Follows	83
4.5.2	Prime Number Factorization	83
4.5.3	Applications of Blockchain Cryptography	84
4.6	Conclusions	85
	References.	85
5	Data Hiding: Steganography and Watermarking	89
5.1	Introduction	89
5.2	Steganography	89
5.2.1	Steganography in Digital Media	91
5.2.2	Steganography Techniques.	92
5.2.3	Steganography Metrics	94
5.3	Watermarking.	94
5.3.1	Watermarking Metrics	95
5.3.2	Watermarking Applications	96
5.4	Visual Cryptography	96
5.5	Conclusions	97
	References.	97
6	Conclusions	99
	Index.	101