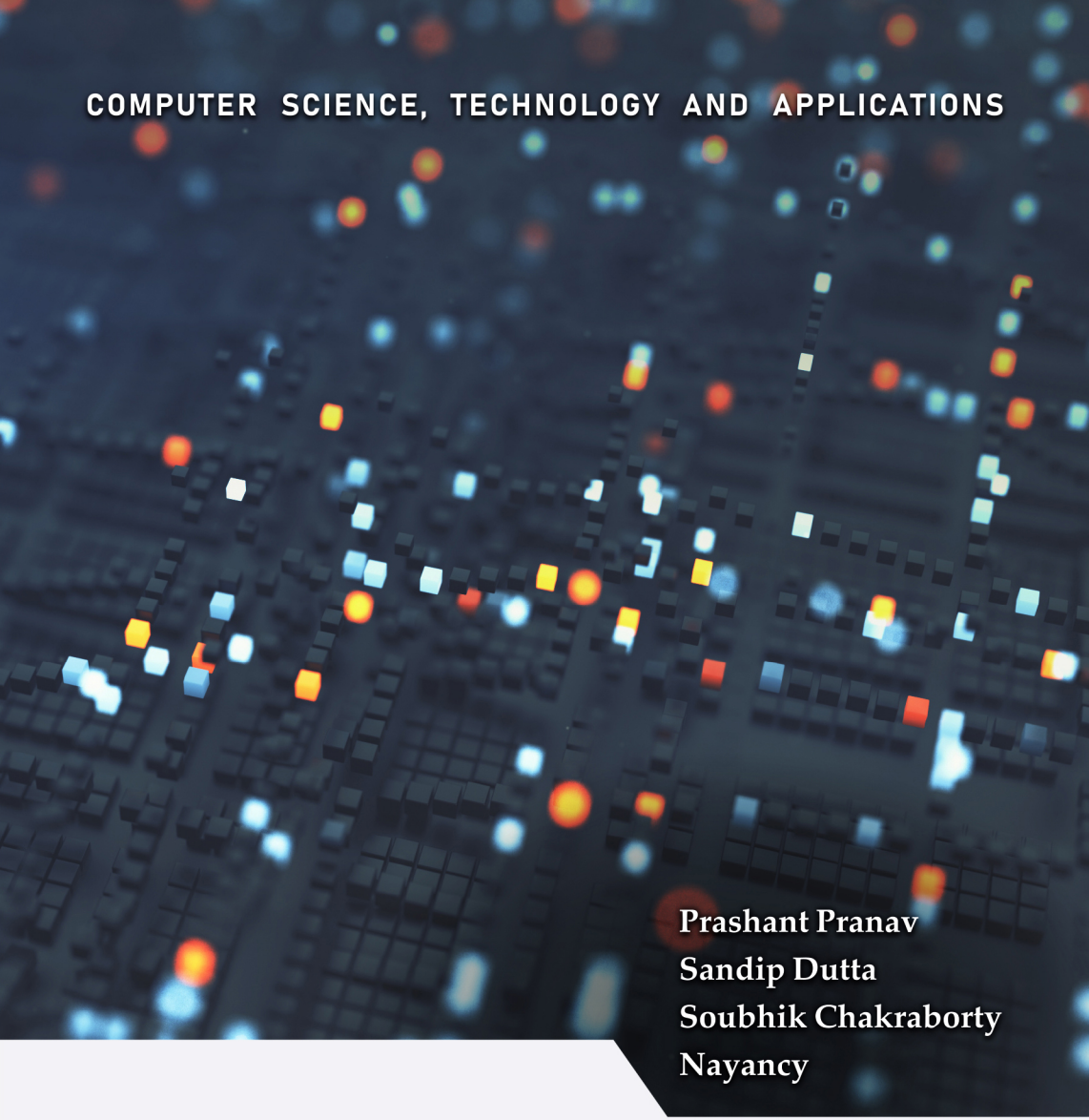

COMPUTER SCIENCE, TECHNOLOGY AND APPLICATIONS

Prashant Pranav
Sandip Dutta
Soubhik Chakraborty
Nayancy

APPLIED CRYPTOGRAPHY

for Researchers and Practitioners

NOVA

Computer Science, Technology and Applications

Computer Science, Technology and Applications

Advances in Bioinformatics and Big Data Analytics
Sujata Dash, PhD, Hrudayanath Thatoi, PhD,
Subhendu Kumar Pani, PhD and Seyedamin Pouriyeh, PhD (Editors)
2023 ISBN: 979-8-88697-693-9 (Hardcover)
2023 ISBN: 979-8-88697-850-6 (eBook)

Demystifying Medical Image Processing Concepts for Design, Implementation and Management with Real Time Case Studies
S. N. Kumar, PhD and S. Suresh, PhD
2023 ISBN: 979-8-88697-737-0 (Softcover)
2023 ISBN: 979-8-88697-796-7 (eBook)

Situational Modeling: Definitions, Awareness, Simulation
Alexander Fridman, PhD
2023 ISBN: 979-8-88697-590-1 (Hardcover)
2023 ISBN: 979-8-88697-725-7 (eBook)

Novel Developments in Computational Intelligence Systems and Their Applications in Multidisciplinary Areas
Manoj Sahni, PhD, José Maria Merigó, PhD,
Ernesto León Castro, PhD, Ritu Sahni, PhD (Editors)
2023 ISBN: 979-8-88697-547-5 (Hardcover)
2023 ISBN: 979-8-88697-585-7 (eBook)

Applications of Artificial Intelligence in the Healthcare Sector
Jyoti Prakash Patra, PhD and Yogesh Kumar Rathore (Editors)
2023 ISBN: 979-8-88697-502-4 (Hardcover)
2023 ISBN: 979-8-88697-541-3 (eBook)

More information about this series can be found at
https://novapublishers.com/product-category/series/computer-science-technology-and-applications/

Prashant Pranav
Sandip Dutta
Soubhik Chakraborty
and Nayancy

Applied Cryptography for Researchers and Practitioners

DOI: https://doi.org/10.52305/OBMR0043.

Library of Congress Cataloging-in-Publication Data

ISBN: 979-8-88697-983-1(eBook)

Published by Nova Science Publishers, Inc. † New York

Contents

Preface ix

Chapter 1 **Introduction to Cryptography**.....1
1.1. Need for Security.....2
1.2. Types of Attacks.....5
1.3. Classification of Cryptography Algorithms.....9
1.3.1. Symmetric Key Cryptography..... 9
1.3.2. Asymmetric Key Cryptography..... 11
1.3.3. Hash Functions..... 13

Chapter 2 **A Note on Traditional and Asymmetric Algorithms**.....17
2.1. Key Exchange Algorithm 18
2.2. History of RSA 20
2.3. El Gamal Algorithm 22
2.4. Elliptic Curve Cryptography: Need of the Hour.....23

Chapter 3 **Symmetric Cryptography: From a Traditional Approach to Recent Trends**.....25
3.1. Most Used Symmetric Cryptography Algorithm 26
3.2. Need of Symmetric Cryptographic Algorithm 31
3.3. PRESENT 80: Need of the Hour.....31
3.4. Traditional vs. Recent Symmetric Cryptographic Algorithm 33

Chapter 4 **Cryptographically Secure Pseudo-Random Number Generator** 35
4.1. Pseudo and True Random Number Generators 35
4.2. Properties of a Cryptographically Secure Pseudo–Random Number Generator 36

4.2.1. Definition 1: Cryptographically Secure Pseudo-Random Bit Generator..... 36
4.2.2. Definition 2: Next-bit Unpredictable..... 37
4.3. A Note on Existing Pseudo–Random Number Generators and Proposing a New Cryptographically Secure Pseudo–Random Bits Generator.....37
4.3.1. Randomized Number of Seconds Between Two Dates 40
4.3.2. Security of Proposed Approach..... 43
4.4. NIST Statistical Suit for Testing the Randomness of the Proposed Cryptographically Secure Pseudo–Random Bits Generator.....43
Appendix: Sequence of Raga Bageshree for the Generation of TPM and Class Matrix.....45

Chapter 5 **Integer Factorization: Can Classical Machines Break the Unbreakable?** 47
5.1. Types of Factorization Problems.....47
5.2. A New Method to Factor Large and Positive Integers From The First Principle.....49
5.2.1. Algorithm 1:Multiplication Subroutine 49
5.2.2. Algorithm 2: Subtraction Subroutine..... 50
5.2.3. Algorithm 3: Division Subroutine..... 50
5.2.4. Algorithm 4: Integer Square Root Subroutine..... 51
5.3. Discussion.....53
5.3.1. Performance Comparison with Existing Factorization Algorithms..... 55

Chapter 6 **Why Lightweight Cryptography after All?**.....57
6.1. Need for Lightweight Cryptographic Protocols.....59
6.2. How Traditional Cryptographic Algorithms Differ from Lightweight Cryptographic Algorithms.....61
6.3. Existing Symmetric Lightweight Cryptographic Algorithms.....62
6.4. Existing Asymmetric Lightweight Cryptographic Algorithms.....64
6.5. Existing Lightweight Key Exchange Algorithms 65

6.6. The Future of Lightweight Cryptography and Its Use in Relevant Domains....66

Chapter 7 **Blockchain Technology and the Hype Behind It**....69
7.1. How Blockchains Are Different from Traditional Ledger-Based Structures....71
7.2. Applications Adopting the Concept of Blockchain Technology....73
7.3. Hype Around Blockchain Technology and the Reason Behind It....76
7.4. How Blockchain Technology Is Going to Change the Future of Digital Payments....76

Chapter 8 **Musical Cryptography: An Isolated But Challenging Research Domain**....79
8.1. Securing Voice Communication Using SNC Algorithm....79
8.1.1. Algorithm:Musical Voice Cryptography....81
8.2. Empirical Complexity of the Proposed Approach....83
8.3. Discussion....86

Chapter 9 **Design of a Fuzzy Rule-Based Expert System for Automatic Raga Selection for Cryptographic Applications**....89
9.1. Fuzzy Set and Fuzzy Rule-Based Expert System....90
9.2. Design of a Fuzzy Rule Based Expert System for Automatic Raga Selection for Cryptographic Applications....91
9.3. Discussion....99

Chapter 10 **Conclusion**....101

References 103

Index 109

About the Authors....113

Preface

Cryptography is the art of writing something secretly. Cryptographic algorithms are the basis of carefree transactions over the internet today. Confidential information of a government or private agency or department is secured by cryptography. From doing secure communication to transferring information of national importance, cryptographic algorithms play the sole role in confidentiality. Cryptography is basically a mathematical model used for hiding confidential information. With the advancement in internet technologies and reliance of everyone on the use of internet in day-to-day life, it has become of utmost importance to hide the confidential information shared over the internet in a form that cannot be read by an intruder.

Chapter 1 gives an overview of different types of cryptographic algorithms. Symmetric key cryptography, asymmetric key cryptography and hash functions are discussed in this chapter.

Chapter 2 provides a note and asymmetric cryptographic algorithms. Various algorithms which use two keys to secure communication have been discussed in this chapter. Diffie-Hellman key exchange algorithm, RSA, El Gamal algorithms are discussed with their underlying steps. Also, the chapter provides a sneak into elliptic curve cryptography.

Chapter 3 gives an insight into symmetric cryptographic algorithms. Algorithms such as AES – 128, DES, Blowfish are discussed in this chapter with a brief overview on to PRESENT 80 algorithms more suitable for lightweight applications.

Chapter 4 discusses in depth the cryptographically secure pseudo random number. These numbers are more suitable to be used in cryptographic applications. The chapter also introduces a new concept to produce random numbers which are cryptographically secure using Indian music. Statistical tests are conducted to validate the proposed work.

Chapter 5 deals with the problem of integer factorization. The security of many cryptographic protocols such as RSA depends on this problem. The

chapter also introduces a new approach to factor large and positive integers from the first principal.

Chapter 6 throws some light on the lightweight cryptography. The chapter also discusses various existing lightweight cryptographic algorithms and the benefit and importance of having such protocols.

Chapter 7 introduces the concept of blockchain technology. The chapter also compares the benefits of blockchain technology compared to traditional ledger-based architecture. Hype around the blockchain technology and applications using it are also provided in this chapter.

Chapter 8 discusses musical cryptography. The chapter has proposed a new approach to secure voice communication using Indian music and discusses the usefulness of music in cryptography.

Chapter 9 deals with a fuzzy rule-based system to secure messages suing musical cryptography. The chapter also compares the worthiness of the proposed system with respect to AES and RSA.

Prashant Pranav
Sandip Dutta
Soubhik Chakraborty
and Nayancy

Chapter 1

Introduction to Cryptography

In today's world, where almost all our personal and professional information is stored digitally, the need for cryptography has become more important than ever. Cryptography is the science of securing information by converting it into an unreadable format that can only be decoded with the right key. This is necessary to protect sensitive information from unauthorized access, modification, and theft.

One of the most common applications of cryptography is in securing communication channels. With the rise of the internet and the increasing use of electronic communication, it has become essential to protect information exchanged between parties. Encryption algorithms are used to encode the message, which can only be decoded by the intended recipient who has the right key. This ensures that the message remains confidential and is not intercepted by a third party.

Cryptography is used to secure digital transactions, such as online banking and e-commerce. Encryption algorithms are used to protect sensitive financial information, such as credit card numbers and bank account details, from unauthorized access. This ensures that the transactions remain secure and private, and the customer's information is not compromised.

Cryptography is utilized to protect stored data, such as personal files and documents. Encryption algorithms can be used to protect files and folders from unauthorized access, ensuring that only those with the right credentials can access the information. This is particularly important for businesses, which often store large amounts of confidential data, including financial records, employee data, and trade secrets.

Cryptography is also used in password protection. Passwords are often the first line of defence in securing information, and encryption algorithms can be used to ensure that passwords remain secure. This is particularly important in cases where passwords are used to access sensitive information, such as financial accounts or medical records.

In summary, the need for cryptography has become increasingly important in today's digital world. Encryption algorithms are used to protect communication channels, secure digital transactions, protect stored data, and