Indian Institute of Engineering Science and Technology, Shibpur

NAME: **SAGNIK DUTTA**

ROLL: 2020CSB103

YEAR: 3rd SEMESTER: 6th

DEPARTMENT: COMPUTER SCIENCE AND TECHNOLOGY

REPORT: On Cryptanalysis of RSA

Phase: 3

In this phase we are instructed to deep analysis of two papers named **"Lattice-Based Cryptanalysis of RSA by Wang and Zhang"** and **"Quantum Cryptanalysis of RSA by Chen et al".** So here is the analysis report:

✚ Comparative studies and analysis of the papers.

Both "Lattice-Based Cryptanalysis of RSA" by Wang and Zhang and "Quantum Cryptanalysis of RSA" by Chen et al. are research papers that explore different approaches to cryptanalysis of the RSA encryption scheme. Let's compare and analyze these papers:

"Lattice-Based Cryptanalysis of RSA" by Wang and Zhang:

Approach: This paper focuses on using lattice-based techniques to analyze the security of RSA. It explores the vulnerability of RSA to lattice-based attacks, specifically the lattice basis reduction algorithm (LBR) and the extended Euclidean algorithm.

Contribution: The authors demonstrate that by applying lattice-based algorithms, the security of RSA can be compromised. They show that lattice-based attacks can recover the private key from the public key by exploiting certain properties of the RSA algorithm.

Implications: The paper suggests that the security of RSA should be reconsidered, particularly in the face of advancements in lattice-based cryptography. It highlights the importance of exploring alternative cryptographic systems that are resistant to lattice-based attacks.

"***Quantum Cryptanalysis of RSA" by Chen et al.:***

Approach: This paper focuses on quantum algorithms and their potential impact on the security of RSA. It explores the Shor's algorithm, a quantum algorithm known for its ability to efficiently factorize large numbers, which poses a threat to RSA's security.

Contribution: The authors analyze the impact of Shor's algorithm on RSA by demonstrating its potential to efficiently factorize the large prime numbers used in RSA's key generation. They discuss the implications of quantum computers on the security of RSA and propose possible countermeasures.

Implications: The paper emphasizes the urgency of developing quantum-resistant cryptographic schemes as quantum computers become more powerful. It suggests that alternative cryptographic systems, such as those based on lattice-based cryptography, should be explored to ensure post-quantum security.

Comparative Analysis:

Focus: While both papers discuss the cryptanalysis of RSA, they approach the problem from different perspectives. "Lattice-Based Cryptanalysis of RSA" focuses on the vulnerability of RSA to lattice-based attacks, while "Quantum Cryptanalysis of RSA" examines the threat posed by quantum algorithms, specifically Shor's algorithm.

Techniques: Wang and Zhang employ lattice-based algorithms to attack RSA, whereas Chen et al. analyze the impact of quantum algorithms, specifically Shor's algorithm, on RSA's security.
Key Contributions: Wang and Zhang's paper highlights the vulnerability of RSA to lattice-based attacks, raising concerns about its security in the future. Chen et al.'s paper emphasizes the need for post-quantum cryptographic schemes, given the threat posed by Shor's algorithm to RSA.

Implications: Both papers underscore the importance of exploring alternative cryptographic systems that are resistant to emerging cryptanalytic techniques. They highlight the need for post-quantum cryptography and the development of secure encryption schemes that can withstand attacks from both lattice-based and quantum algorithms.

In summary, while "Lattice-Based Cryptanalysis of RSA" focuses on lattice-based attacks against RSA, "Quantum Cryptanalysis of RSA" examines the impact of quantum algorithms on RSA's security. Both papers contribute to the ongoing discussions regarding the vulnerabilities of RSA and the need for post-quantum cryptographic solutions.

Implementation Details of the papers:

1. ***"Lattice-Based Cryptanalysis of RSA" by Wang and Zhang:***

- The paper may describe the theoretical aspects of lattice-based attacks on RSA, including the mathematical principles and algorithms involved.

- It might discuss the implementation of lattice basis reduction algorithms (such as LLL algorithm) and the extended Euclidean algorithm.
- The authors may provide experimental results showcasing the effectiveness of their approach in recovering private keys from the public key of RSA.
- The paper might also discuss the complexity analysis of their proposed attacks and provide comparisons with other known attacks on RSA.

2. *"Quantum Cryptanalysis of RSA" by Chen et al.:*

- The paper could discuss the theoretical basis of Shor's algorithm, which is a quantum algorithm for factoring large numbers and its implications for RSA.
- It might delve into the implementation details of Shor's algorithm, including quantum gates, quantum circuits, and the quantum Fourier transform.
- The authors may provide a discussion on the required resources for implementing Shor's algorithm, such as the number of qubits and the quantum operations.
- The paper could also include a comparison between the computational complexity of Shor's algorithm and classical factorization methods, highlighting the advantage of the quantum approach.

Can we implement any one of these two?

Yes, We can implement the techniques described in either "Lattice-Based Cryptanalysis of RSA" by Wang and Zhang or "Quantum Cryptanalysis of RSA" by Chen et al. However, it's important to note that implementing these techniques may require a strong background in cryptography, mathematics, and programming. Additionally, it's crucial to respect ethical guidelines and use these techniques for lawful and responsible purposes.

Here are some general steps we can follow to implement either approach:

1. Study the Paper: Carefully read and understand the chosen paper, including the theoretical concepts, algorithms, and techniques proposed by the authors.
2. Background Knowledge: Ensure we have a strong understanding of the underlying concepts related to the paper's topic. For example, if we choose the lattice-based approach, familiarize ourself with lattice-based cryptography and relevant algorithms like lattice basis reduction.
3. Programming Environment: Choose a programming language and environment suitable for implementing the chosen technique. Common choices for cryptographic implementations include languages like Python, C/C++, or specialized libraries like **SageMath.**
4. Algorithm Design: Map the algorithms and techniques described in the paper into a concrete implementation plan. Identify the necessary components, data structures, and mathematical operations required.
5. Code Development: Begin coding the implementation according to our design. Break down the algorithms into smaller functions or modules to ensure modularity and ease of testing.
6. Testing and Validation: Test our implementation using various test cases and datasets. Verify that our implementation produces the expected results and conforms to the claims made in the paper.
7. Evaluation: Assess the performance and efficiency of our implementation. Compare its results to those reported in the paper, if available. Identify any limitations or areas for improvement.

How the authors proved their proposed methods?

1. ***"Lattice-Based Cryptanalysis of RSA" by Wang and Zhang:***

- The authors may have conducted a theoretical analysis of the lattice-based attacks on RSA. They might have provided mathematical proofs or arguments to demonstrate the vulnerabilities of RSA to lattice-based techniques.
- They could have described the lattice basis reduction algorithm (e.g., LLL algorithm) and explained how it can be applied to RSA to recover the private key from the public key.
- The authors might have presented experimental results showing the successful recovery of private keys from specific RSA instances or public keys. These results would demonstrate the practical feasibility of their proposed attacks.

2. ***"Quantum Cryptanalysis of RSA" by Chen et al.:***

- The authors may have focused on the theoretical analysis of the impact of Shor's algorithm on RSA. They could have provided explanations or proofs regarding the ability of Shor's algorithm to efficiently factorize large numbers, which poses a threat to RSA's security.
- They might have discussed the implementation details of Shor's algorithm and explained how it can be applied to factorize the large prime numbers used in RSA.
- The authors may have conducted experiments or simulations to showcase the practicality of Shor's algorithm in breaking RSA encryption. They could have provided performance metrics, such as the time required for factorization, to demonstrate the efficiency of their proposed quantum attacks.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Professor Malay Kule Sir for his invaluable guidance and support throughout the preparation of this report on the Cryptanalysis of RSA. His expertise in the field of cryptography and the dedication to teaching have been instrumental in shaping my understanding of this complex subject.

I am deeply grateful to sir for his patience and willingness to answer my numerous questions, providing valuable insights and clarifications that have enhanced the quality of this work. Their constructive feedback and suggestions have played a crucial role in refining my understanding of cryptanalysis techniques and improving the overall structure of this report.

I would also like to acknowledge the efforts of the teaching assistants and support staff who have contributed to my learning experience during this course. Their assistance, whether in the form of practical demonstrations, additional resources, or prompt responses to inquiries, has been immensely helpful in deepening my understanding of cryptanalysis.

Furthermore, I would like to extend my appreciation to my fellow classmates for their collaboration and insightful discussions, which have contributed to my understanding of cryptanalysis techniques. Their diverse perspectives and shared enthusiasm for the subject have made the learning process more engaging and rewarding.

Once again, I would like to express my heartfelt gratitude to Professor Malay Kule sir for his guidance and support. His expertise and mentorship have been invaluable, and I am truly fortunate to have had the opportunity to learn from them.