Contribution ID: **13** Type: **not specified**

Breaking RSA and picking up the pieces

Thursday 27 March 2025 09:00 (1 hour)

As quantum computers advance, they pose a significant threat to our current cryptographic infrastructure, particularly RSA encryption. This presentation will explore how RSA can be broken using Shor's algorithm and examine the landscape of post-quantum encryption algorithms.

Presentation Overview

Introduction to RSA and Its Importance in Modern Cryptography

- Brief history of RSA
- Current widespread use in secure online transactions and communications

The Quantum Threat: Shor's Algorithm and Its Impact on RSA

- Explanation of Shor's algorithm
- How quantum computers can factor large numbers exponentially faster than classical computers
- Implications for RSA security

Post-Quantum Cryptography: An Overview

- Introduction to post-quantum cryptographic algorithms
- Types of post-quantum cryptography (lattice-based, code-based, multivariate polynomial, hash-based signatures)

Standardization Efforts: NIST's Post-Quantum Cryptography Project

- Overview of NIST's standardization process
- Selected algorithms (CRYSTALS-Dilithium, FALCON, SPHINCS+, CRYSTALS-Kyber)
- Challenges in standardization and implementation

Implementation Considerations for Post-Quantum Algorithms

- Integration into existing cryptographic libraries
- Performance comparisons with classical algorithms
- Security analysis and known vulnerabilities

Key Takeaways

1. Understanding of the quantum threat to RSA and current public-key cryptography
2. Knowledge of post-quantum cryptographic algorithms and their types
3. Insights into implementation challenges and migration strategies
4. Insights into preparing for the post-quantum era in cybersecurity

Number of lecture hours

1

Number of exercise hours

0 (no exercises)

Attended school

tCSC on Security 2023 (Split)

Author: SHARMA, Vasvi

Presenter: SHARMA, Vasvi