RSA Cryptography

CS 532 - Cryptography & Data Security
Kelly Powell & Taylor Hunter

Introduction to RSA

What is RSA?

- Public-key crypto system from **1978**
- Made by Rivest, Shamir, and Adleman
- Big deal: You are able to encrypt things without having to share a secret key first

Why was this Important?

- Before RSA: Everyone had to use the same secret key
- Problem: How are you able to safely share the key?
- RSA fixes this issue

The Math Idea

- Easy direction
- Hard direction
- When done correctly this asymmetry is what makes RSA secure

Connection to Cryptography Field

Fixing the Key Problem

- Old crypto
- Scaling quadratically
- Difference with RSA

Where Do We Use RSA Today?

- HTTPs websites
- Code signing
- Email encryption
- Digital Certificates
- IoT devices

Why We’re Studying This?

- Good example of math theory working in practice
- Shows concepts like modular arithmetic, prime numbers, and computational complexity
- Shows how theory vs. implementation can go wrong

How RSA Works

Setting Up Keys

1. Pick two random prime numbers: **p & q**
2. Multiply them: **$n = p \times q$**
3. Calculate **$\varphi(n) = (p-1)(q-1)$**
4. Pick **e**
5. Find **d** where **$d = e^{-1} \pmod{\varphi(n)}$**

Actually Using RSA

- Encrypt: $\mathbf{c = m^e \bmod n}$
- Decrypt: $\mathbf{m = c^d \bmod n}$

What is Shared vs. Kept Secret

- Public key: **(e,n)**
- Private key: **(d, n)**
- Security depends on **d & e**

Main Issues/Problems

Keys Too Small

- Old 512-bit keys can be broken now
- Need at least 2048 bits
- Small keys have no change

Bad Random Numbers

- 0.5% of internet RSA keys can be easily broken
- Devices use bad random number generators
- Two different keys cannot use the same prime

Implementation Mistakes

- Using e = 3 without proper padding
- PKCS

Speed Issues

- RSA is slow
- Only for encrypting small things
- Not practical for large files

Quantum Computers

- Shor’s algorithm
- Something we need to plan for

Weak Implementation Vulnerabilities

Real-World Consequences

- Complete Security Failure
- IoT vulnerabilities
- Pattern Detection

Common Implementation Errors

- Identical random seeds across devices
- Insufficient entropy during key generation
- Poorly chosen primes
- Incorrect padding implementations

Case Studies

- Heninger and his colleagues
- IoT security failures
- Academic Demonstrations

Hands-On Demonstration

DEMO of Weak RSA

GitHub Repo: https://github.com/Taylor-Hunter/RSA_Project

What We Learned

RSA Is Still Important

- Still used everywhere
- Good for learning how crypto theory works in practice
- Many systems still depend on it working correctly

What Makes RSA Secure

- Key size matters
- Random numbers need to be actually random
- Implementation details matter
- Keep up with security recommendations as they change

Looking Forward

- Quantum computers will eventually break all RSA
- Will need post-quantum crypto
- RSA currently works if done right
- Worth understanding

References

Almazari, Mahmoud M., et al. "RSA Private Keys and the Presence of Weak Keys: An Evaluation." Journal of Discrete Mathematical Sciences and Cryptography, July 2022.

Boneh, Dan. "Twenty Years of Attacks on the RSA Cryptosystem." Notices of the AMS, 2007.

Gerjuoy, Edward. "Shor's Factoring Algorithm and Modern Cryptography." American Journal of Physics, vol. 72, no. 5, 2004.

Heninger, Nadia, et al. "Detection of Widespread Weak Keys in Network Devices." USENIX Security Symposium, 2012.

Just, Jiri, and John Coffey. "An Assessment of Attacks Strategies on the RSA Public-Key Cryptosystem." International Institute of Informatics and Systemics, 2009.

Kilgallin, Jonathan, and Ross Vasko. "Factoring RSA Keys in the IoT Era." IEEE/Keyfactor, 2019.

References

Maitra, Subhamoy, and S. Sarkar. "Revisiting Wiener's Attack: New Weak Keys in RSA." Lecture Notes in Computer Science, vol. 5222, Springer, 2008.

Paar, Christof, Jan Pelzl, and Tim Güneysu. Understanding Cryptography: From Established Symmetric and Public-Key Primitives to Advanced Protocols. 2nd ed., Springer Spektrum, 2024.

Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM, vol. 21, no. 2, 1978.

Ruzai, W. N. A., et al. "Concurrent Factorization of RSA Moduli via Weak Key Conditions." AIMS Mathematics, vol. 9, no. 5, 2024.