Attacks on RSA

Karam Gill
karamsgill12@gmail.com

Euler Circle

July 13, 2025

What is RSA?

Rivest-Shamir-Adleman (RSA)

- Alice is communicating with Bob, Charlie is eavesdropping

How Does RSA Work?

- Public Key: (N, e)
- Private Key: (N, d)
- RSA modulus $N = pq$

How Does RSA Work?

How do we generate numbers e and d?

- We generate e such that $\gcd(e, \phi(N)) = 1$
- Then we generate d such that $ed \equiv 1 \pmod{\phi(N)}$

Encryption and Decryption

How does Bob receive the message from Alice?

- Alice computes ciphertext $C \equiv M^e \pmod{N}$ then sends to Bob
- Bob decrypts the ciphertext calculating $C^d \equiv M \pmod{N}$ so Bob receives the legitimate message

Attacks on RSA

We will talk about three attacks on RSA.

- Common Modulus Attack
- M. Wiener Attack
- Random Faults

Common Modulus Attack

The first attack we will talk about is the Common Modulus Attack.

- Alice's Keys: $(N, e_a), (N, d_a)$
- Bob's Keys: $(N, e_b), (N, d_b)$

In the next slide we will prove a key theorem.

Key Theorem

Theorem 1: Given the private key d and the public key (N, e) one can efficiently factor N and given the factorization of N one can efficiently find the private key d.

- Bob finds p, q using d_b
- Bob finds d_a using p, q

Micheal J.Wiener Attack

Theorem 2: Let $N = pq$ with $q < p < 2q$. Assume that the private exponent $d < \frac{1}{3}N^{\frac{1}{4}}$. Given the public key (N, e) with $ed \equiv 1 \pmod{\phi(N)}$, Charlie can efficiently recover the private key d.

Proof

- Let k be such that $ed - k\phi(N) = 1$
- Dividing by $d\phi(N)$ yields $\left|\frac{e}{\phi(N)} - \frac{k}{d}\right| = \frac{1}{d\phi(N)}$
- So $\frac{k}{d}$ and $\frac{e}{\phi(N)}$ are approximations of each other
- Note that $\phi(N) = (p-1)(q-1) = pq - p - q + 1 = N - p - q + 1$
- Also $p + q - 1 < 3q < 3\sqrt{N}$
- Thus $\phi(N) > N - 3\sqrt{N} \implies |N - \phi(N)| < 3\sqrt{N}$

Proof

- We will use the key result $|N - \phi(N)| < 3\sqrt{N}$
- We can see that $\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed-kN}{dN}\right| = \left|\frac{ed-k\phi(N)-kN+k\phi(N)}{dN}\right| = \left|\frac{1-k(N-\phi(N))}{dN}\right|$
- Note that $k\phi(N) < ed, e < \phi(N) \implies k < d < \frac{1}{3}N^{\frac{1}{4}}$
- Thus $\left|\frac{e}{N} - \frac{k}{d}\right| \leq \frac{3k}{\sqrt{N}d} \leq \frac{N^{\frac{1}{4}}}{\sqrt{N}d} = \frac{1}{N^{\frac{1}{4}} \cdot d} < \frac{1}{2d^2}$.

Approximation Relation

- $\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$
- The bound is a classic approximation relation
- We test all $\frac{k}{d}$ that approximate $\frac{e}{N}$
- By the approximation relation we have to test $\log_2(n)$ values

Random Faults

This attack is more about faults in the system rather than a breaking of the RSA.

- Compute M^d mod p, q
- Use CRT to get $M^d \pmod{N}$
- This process is called CRT speedup and is 4 times faster than normal
- However, this method can lead to devastating consequences if executed poorly

Process

Before we can jump into the attack, we must talk about how we compute the ciphertext $\mod p$ and $\mod q$. Firstly, we compute

$$C_p \equiv M^{d_p} \pmod{p}, C_q \equiv M^{d_q} \pmod{q}$$

where we define

$$d_p \equiv d \pmod{p-1}, d_q \equiv q \pmod{q-1}.$$

Ciphertext

How do we compute the ciphertext from here? In order to get the ciphertext C, we compute $C \equiv T_1 C_p + T_2 C_q \pmod{N}$ where

$$T_1 \equiv 1 \pmod{p}, T_1 \equiv 0 \pmod{q}$$

and

$$T_2 \equiv 0 \pmod{p}, T_2 \equiv 1 \pmod{q}.$$

Verification

First we have to verify that the original ciphertext is actually congruent to what we listed in the previous slide. We will prove that this equation holds both $\pmod p$ and $\pmod q$. Taking $\pmod p$, we have

$$T_1 C_p + T_2 C_q \equiv T_1 C_p \equiv C_p \equiv C \pmod p.$$

Furthermore,

$$T_1 C_p + T_2 C_q \equiv T_2 C_q \equiv C_q \equiv C \pmod q.$$

Thus $T_1 C_p + T_2 C_q \equiv C \pmod N$.

Random Faults

We will now discuss the process of the attack.

- C_q incorrectly encrypted: resultant C'_q
- False $C' \equiv T_1 C_p + T_2 C_q \pmod{N}$
- Charlie checks veracity of ciphertext

Taking the GCD

What is the big deal of Charlie knowing the ciphertext is false?

- $C'^e \equiv M \pmod{p}$ but $C'^e \not\equiv M \pmod{q}$
- $\gcd(N, C'^e - M)$ reveals p

Future of RSA

What does the future of the RSA cryptosystem look like?

- Short Term: Key lengths increase due to computational development
- Medium Term: RSA will be used less practically
- Long Term: RSA will likely be broken

RSA Attacks

I will list the attacks covered in my paper,

- Blinding Attack
- Common Modulus Attack
- Wiener Attack
- Meet in the Middle Attack
- Hastad's Broadcast Attack
- Coppersmith's Attack
- Partial Key Exposure Attack
- Franklin-Reiter Attack
- Random Faults
- Timing Attacks
- Bleichenbacher Attack
- Coppersmith Short Pad Attack
- Power Analysis
- Cold Boot Attack

Questions

Any questions?