Rivest-Shamir-Adleman (RSA) Cryptosystem

"No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems very unlikely that anyone will do so for many years."

– A Mathematician's Apology by G.H. Hardy, 1940

"Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve." – Edgar Allan Poe

Actually, the RSA cryptosystem:

1) Is based on number theory.

2) Widely used and has resisted decades of attack.

3) The encryption method is public!

Rivest-Shamir-Adleman (RSA) Cryptosystem

Setup:

1. Choose distinct primes p and q and take $n = p \cdot q$
2. Choose an $e \in \mathbb{N}$ such that $\gcd(e, \phi(n)) = 1$.
3. Take $d = e^{-1}$ in $\mathbb{Z}_{\phi(n)}$ so that $de \equiv 1 \bmod \phi(n)$.

Public key: n, e Private key: d Other private info: p, q

Message: $m \in \{0, 1, \dots, n-1\}$

Encryption: Send $x = m^e \bmod n$ Anyone can do this as n and e are public!

Decryption: Compute $x^d \bmod n$ Only you know d.

This decryption works as

$$x^d \bmod n = (m^e)^d \bmod n = m^{de} \bmod n = m^{de \bmod \phi(n)} \bmod n$$
$$= m \bmod n = m$$

RSA Security

Is RSA secure?

- If an adversary can factor n by finding p and q, they can compute $\phi(n) = (p-1)(q-1)$ and then find $d = e^{-1}$ in $\mathbb{Z}_{\phi(n)}$.
- Other minor issues:
  - A handful of messages such as $m=0$ or $m=1$ are not very secure.
  - If the adversary can guess m, they can confirm it by checking if $x = m^e \bmod n$.
- Once these issues are patched, factoring n is the only way we know of to break RSA.
- Is factoring n hard?
  - We don't know for sure, but factoring has resisted hundreds of years of attack by classical algorithms, so we conjecture it's hard for classical algorithms.
  - There is a quantum algorithm, Shor's algorithm, for factoring so RSA can be broken by a quantum computer.