Prime Numbers and RSA

Alyssa Byrnes

Motivation

- Primes are a common topic among computer scientists and mathematicians.
- This is because they have many useful mathematical properties!
- One popular application is asymmetric cryptography, which we will talk about later.

Prime vs. Composite

A positive integer is **composite** if it can be written as the product of two smaller, positive integers.

$$N \text{ is composite if and only if}$$
$$\exists\, a, b \in (1, N), N = a \times b$$

A number is **prime** if it is not composite.

In other words, its only factors are 1 and itself.

The Fundamental Theorem of Arithmetic

It has the word “fundamental” in it, so you know it’s important!

Fundamental Theorem of Arithmetic: Every number can be written as a unique product of prime numbers

Examples (Not a proof!):

- $100 = 4 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5$
- $2020 = 2 \cdot 2 \cdot 5 \cdot 101$

Activity

At home, try to come up with an algorithm that finds the prime factors of a given number, N. Then use it to try to factor the numbers 2020 and 2021.

Runtime of Prime Factorization

A number that is a product of two large primes can take an extremely long time to factor.

Consider the number

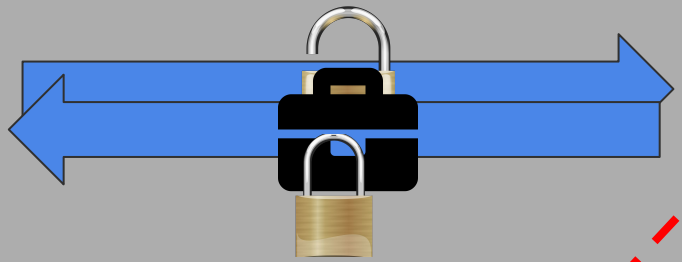
```
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357
```

It is 617 digits long, and 2048 bits. It is also the product of two large primes!

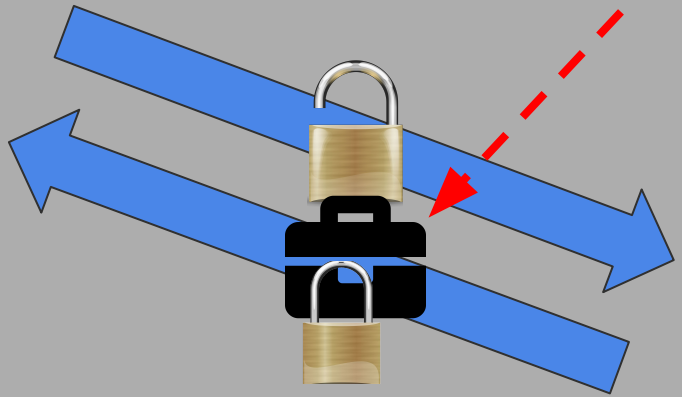
It is estimated that it would take a classical computer around 300 trillion years to factor this![QL]

This is the foundation of RSA Cryptography.

Alice



Bob



Chris

Terminology

“Public Key”
Used to **encrypt** messages

“Private Key”
Used to **decrypt** messages

Important Rules:

1. The act of locking and unlocking (aka encrypting and decrypting) our lock shouldn’t alter the contents of the message.
2. Observing the public key can’t give you any information about the private key

RSA Encryption and Decryption

Part of your “public key” is a number N that is a multiple of two numbers, p and q.

Your “private key” is dependent on p and q, so they need to be difficult to figure out.

Now we know how to make p and q difficult to figure out… make them prime! Then it will be near impossible to factor N and find out p and q!

Modular Encryption

We are going to to encode and decode a number x.

Public key: (e, N)

Private key: (d, N)

Encrypt: $y = x^e \bmod N$

Decrypt: $x = y^d \bmod N$

Important Rules:

1. The act of locking and unlocking (aka encrypting and decrypting) our lock shouldn't alter the contents of the message.

$$(x^e)^d \bmod N = x$$

2. Observing the public key can't give you any information about the private key

Given e and N,

someone shouldn't be able to figure out d.

RSA - picking N, e, and d

(e, N)  (d, N) $\quad N = p \times q,\ p$ and q are prime

Fact:

If $r \equiv 1 \pmod{(p-1)(q-1)}$,

then $x^r \bmod N = x$.

So, we define e and d such that

$$e \times d \equiv 1 \pmod{(p-1)(q-1)}$$

$$(x^e)^d \bmod N = x$$

RSA Example

$$p = 3,\ q = 11,\ N = 33,\ (p-1)(q-1) = 2 \times 10 = 20$$

$$e = 7,\ d = 3, 3 \times 7 \bmod 20 = 1$$ 

Encrypting the number 2 :

$$y = 2^7 \bmod 33 = 128 \bmod 33 = 29$$

Decrypting the number 29 :

$$y = 29^3 \bmod 33 = 24389 \bmod 33 = 2$$

Why is this secure?

What an attacker knows:

$$e \text{ and } N,$$

$$(x^e)^d \bmod N = x,$$

$$e \times d \equiv 1 \pmod{(p-1)(q-1)}$$

$$N = p \times q$$

Why is this secure?

What an attacker knows:

e and N,

$$(x^e)^d \bmod N = x,$$

$$e \times d \equiv 1 \pmod{(p-1)(q-1)}$$

$$N = p \times q$$

Could be true for many values of d,

$29^3 \bmod 33 = 2,$

but also

$29^{13} \bmod 33 = 2,$

$29^{23} \bmod 33 = 2,$

$29^{33} \bmod 33 = 2,$

$29^{43} \bmod 33 = 2,$

$\ldots$

Why is this secure?

What an attacker knows:

e and N,

$(x^e)^d \bmod N = x$,

$e \times d \equiv 1 \pmod{(p-1)(q-1)}$

$N = p \times q$

Don’t know p or q

Why is this secure?

What an attacker knows:

e and N,

$(x^e)^d \bmod N = x$,

$e \times d \equiv 1 \pmod{(p-1)(q-1)}$

$N = p \times q$ ← Hard to find p or q

Given e and N,
someone shouldn't be able to figure out d.

Takeaways

Primes are important!

- They have many useful mathematical properties.
- Products of large primes are hard to factor.

The basic reasoning behind RSA and why it works.

- (Future lesson: generating keys)

Thank you for your attention!