Admin

- HW3 due today
- I'll be faster grading after this week
- I'll be strict w/ the take home deadline; Th wk10 lights

Cryptography

Goal. Communicate securely over insecure channels.

A good encryption standard should ensure

- Secrecy - no one can read it but those who are allowed
- unmodifiability - it cannot be modified in transit
- authentic endpoints - Sender and receiver can be assured of each other's identity (possibly pseudonymous)

We focus on secrecy here.

Naive ciphers:

- Fix a permutation of the alphabet and agree on it before hand. Scramble messages thus. This is the Caesar cipher.

Faults: - Easy to decode (repeated letters)
- once decoded, all previous messages are decodable
- must agree beforehand!
  - Is it possible for strangers to communicate securely?

- Pig latin

Caesar cipher is Symmetric: both parties use the same "key".

In the 70's Diffie and Hellman revolutionized cryptography by a method for two strangers to agree on a public key.

Later on Rivest, Shamir, and Adleman created a "public key" cryptosystem (RSA) which allows messages to be transmitted securely without any prior agreement or shared key.

Rmk. Symmetric encryption is often faster for 2 peers seeking to communicate, so nowadays your browser will use a key-exchange alg Diffie-Hellman to generate a shared secret, then use a

Diffie-Hellman

Lemma, $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclic

pf. If x^{d-1} $d < p-1$ ✳

A	B	M
a	b	g
g^a	g^b	g^a
g^{ab}	g^{ab}	g^b

$\log_g : \langle g \rangle \longrightarrow \mathbb{Z}/p-1\mathbb{Z}$

$g^1 \longrightarrow 1$

Math is declarative } SICP

CS is imperative }

RSA

Let p, q distinct primes.

$n = pq$ $\rightarrow$ the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$

Compute $\operatorname{lcm}(p-1, q-1) = k$

Pick e s.t. $\gcd(e, k) = 1$

$1 < e < k$

Compute $d \equiv e^{-1} \bmod k$

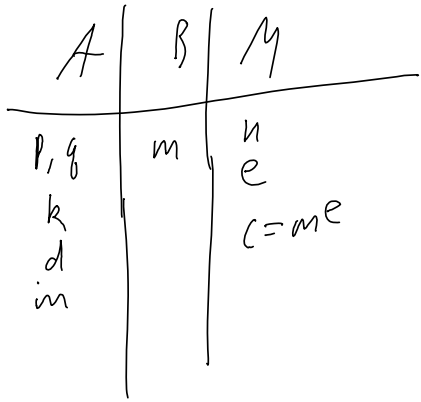
public key: (n, e) Rmk. They don't know p, q!

private key: d

Say your message m is encoded as an integer (ASCII, unicode, etc) s.t. $0 \le m < n$,

The <u>cipher</u> is m^e in $\mathbb{Z}/n\mathbb{Z}$

To decrypt, m^e, raise it to the d^{th} power



Attacks: Computing $e^{-1} \bmod k$