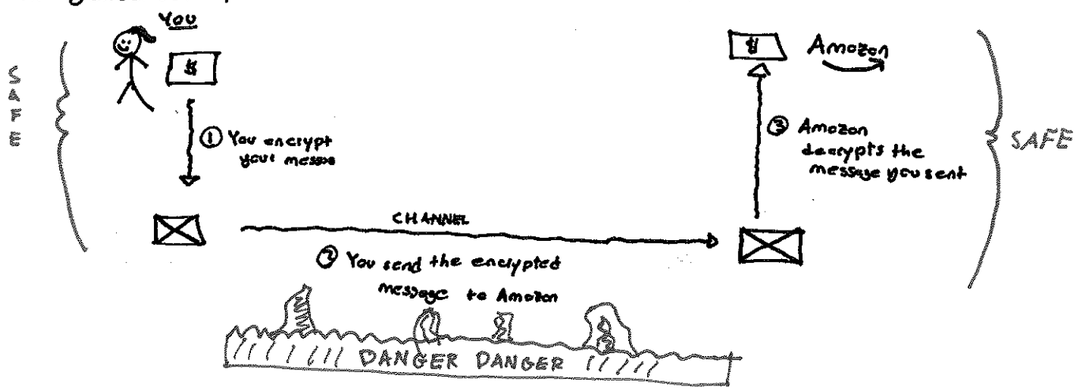
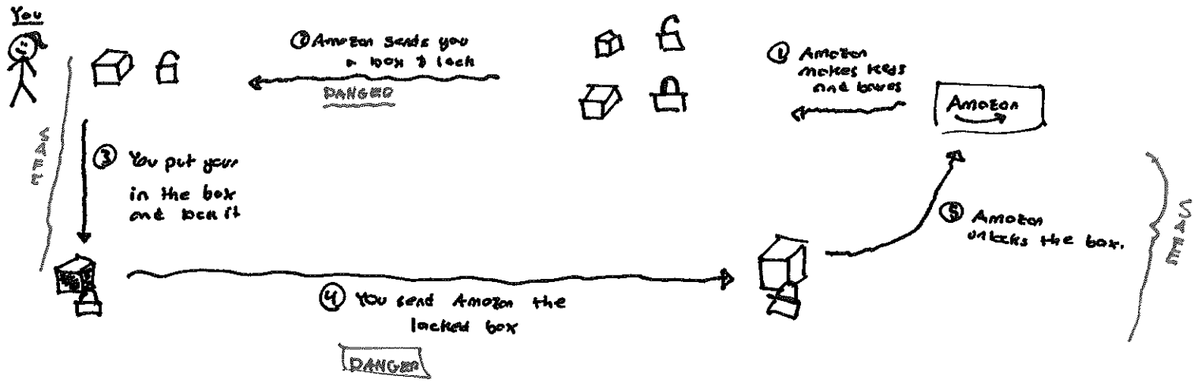
- Q: How can we communicate data securely?
  - ↳ Data has a lot of meanings in the real world:
    - Credit card Information
    - Bank Information
    - Text Messages.
    - etc.

- The general set up of this sort of problem is a follows



- Q: I am missing one critical step of this algorithm for it to make sense, what is it?
  - ↳ A: How does Amazon know how to decrypt the message?
    - ↳ Note we cant sent instructions through the channel or others will know how to decrypt our message to

- Public Key Cryptography:
  - Step # 1: Amazon makes a bunch of "boxes" and "locks"
  - Step # 2: Amazon sends you a ~~bunch of~~ boxes and a unlocked lock.
  - Step #3: You put your message in the box and lock it with the lock amazon sent you.
  - Step #4: You send amazon their locked box back.
  - Step #5: Amazon un-locks the box.



- WANT TO EXPLORE HOW WE MAKE THESE KEYS.

- Def: A number is prime if its only divisors are 1 and itself.

- Ex: which of the following are prime:
  - 7
  - 10
  - 35
  - 37
  - 1009
  - 1011
  - $2,147,483,647$ (1772)
  - $60701 = 101 \cdot 601$.

- Def: If n is a natural number we say

$\phi(n)$ = # of natural numbers less than n s.t. they have no common factors with n → we say such #'s are coprime.

- Ex: $\phi(5)$
  - $\phi(7)$
  - $\phi(p)$ where p is prime.

- Def: Let A, B, C be integers then

$A \equiv B \bmod C \iff C$ divides $A - B \iff$ the remainder of A/C is B

↳ Recall by the divison algorithm we can write

$$A = qC + r$$

(r is the remainder.)

- Ex: when is $A \equiv 0 \bmod 2$? $A \equiv 1 \bmod 2$?
  - Is there a d s.t. $(d \cdot 17) \equiv 1 \bmod 3120$?
  - $2^5 \bmod 5$, $7^5 \bmod 5$, $11^3 \bmod 3$, $3^{11} \bmod 11$?

• Key Creation:

1) Pick prime #'s $p \neq q$ • $p = 13$, $q = 17$

~~Jumbermapping~~

• $n = 13 \cdot 17 = 221$

3) Compute $\phi(p \cdot q)$ • $\phi(221) = 192 = 2^6 \cdot 3$

↳ Ex this equals $(p-1)(q-1)$.

• $e = 7$

5) Choose $1 < e < \phi(p \cdot q)$ coprime to $(p-1)(q-1)$ • $7d = 192q + 1$

Let $q = 2 \Rightarrow 7d = 384 + 1$

$\Rightarrow d = 55$.

4) Choose d s.t

$d \cdot e \equiv 1 \bmod \phi(n)$.

• Def: • The pair $(p \cdot q, e)$ is the public key. • $(221, 7)$
(Everyone knows)

• The pair $(p \cdot q, d)$ is the private key. • $(221, 55)$
(Only Amazon knows)

• Q: How do we use these keys?

• Step #1: We convert our message to a number $m < p \cdot q$.

↳ This is easy and can be done many ways.

• Step #2: Compute $m^e \bmod p \cdot q = c$.

• Step #3: Send amazon c.

• On the other end amazon needs to recover m from c and their private key.

• Step 1: Compute $c^d \bmod p \cdot q$.

• Claim: $m \equiv c^d \bmod p \cdot q$

• Ex: - Let us use the simple scheme that

$$A=1,\ B=2,\ 3=C,\ D=4,\ E=5$$

so that

$$BAD = 214.$$

• If we compute $214^7 \bmod 221 \equiv 124$.

• The claim says that $124^{55} \bmod \equiv 214$, which it is!

• Great, we have a way to encrypt and decrypt messages, and all our these steps are easy for computers to do, but is this method secure?

• EXERCISE: Encode a 4 letter word using the scheme

$$A=1,\ B=2,\ C=3,\ \ldots$$

and using primes $P, q < 1000$. I AM GOING TO LEAVE. WHEN I COME BACK I want to see your encrypted message & your public key! LET'S SEE IF ITS SECURE.

• Answer: To decrypt your message I need

$$\text{YOUR PUBLIC KEY} \overset{?}{=} d.$$

$$\Leftrightarrow \quad \text{I JUST need } \underline{d}.$$

• well I know you picked primes P & q, and e, & d, s.t.

$$e \cdot d \equiv 1 \bmod [(P-1)(q-1)]$$

$$\Leftrightarrow e \cdot d \equiv N(P-1)(q-1) + 1. \qquad \text{for some } N \in \mathbb{Z}.$$

Q: What is $e \cdot d \bmod [P-1]$? $e \cdot d \bmod [q-1]$?

• This means to find d I just need to find d s.t.

$$d \cdot e = N(P-1) + 1$$

$$d \cdot e = N(q-1) + 1$$

In fact, we can do this very easily.