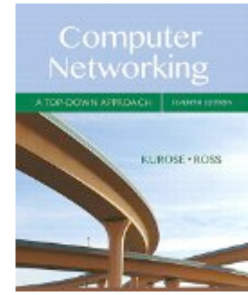
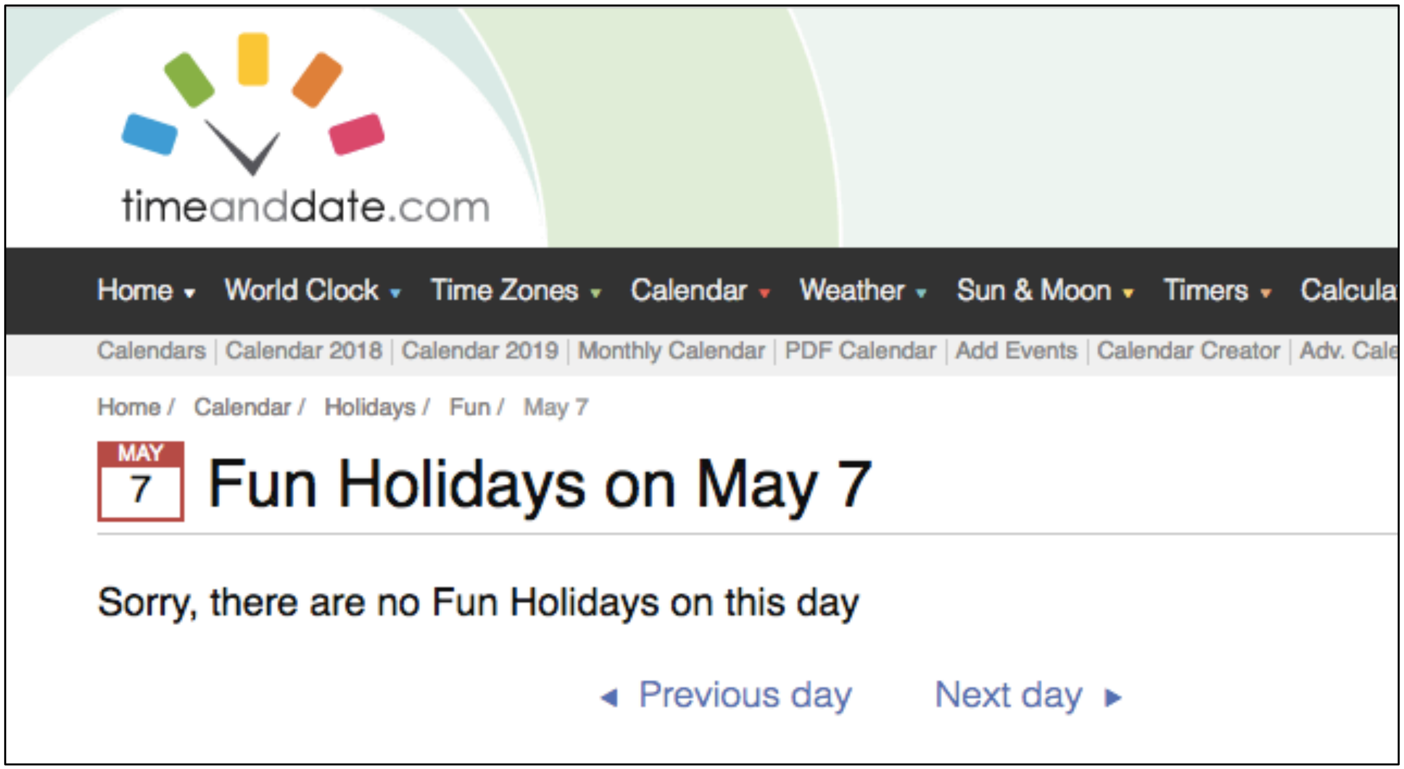
COMP 375: Lecture 39



- **News & Notes:**
  - Quiz #9 in class today
  - Final exam: Friday, May 18 @ 11AM
- **Reading (Wed, May 9)**
  - Sections 8.{6, 7} (Transport and Network Layer Security)

Quiz #9

- Closed book. Closed notes.

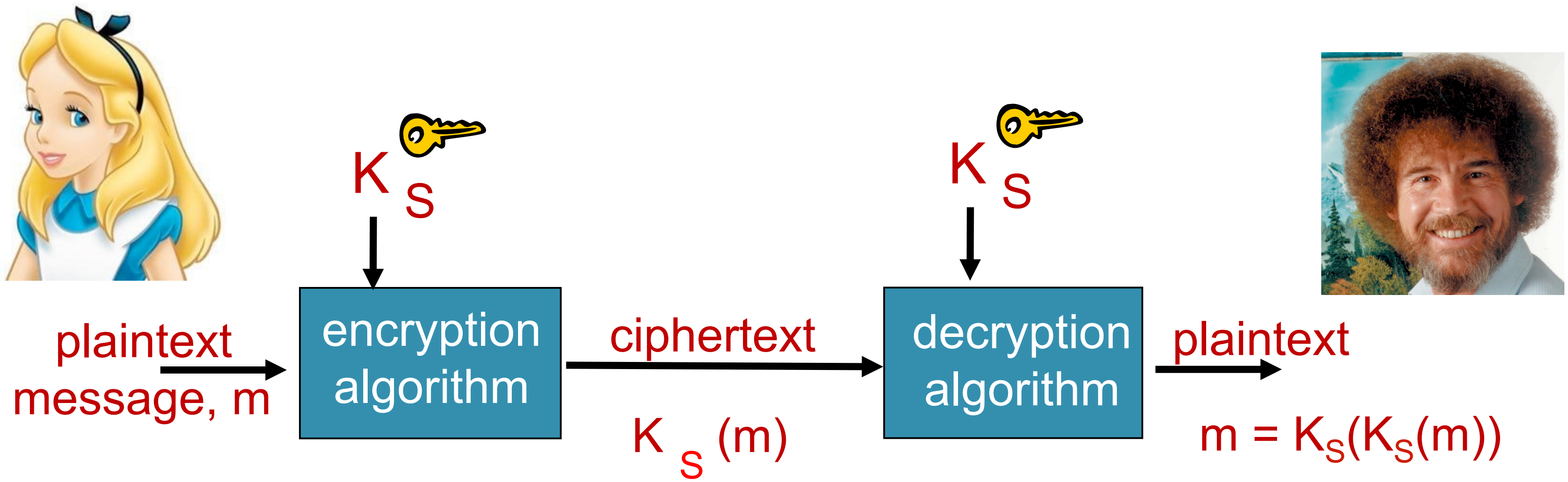


What about "Last COMP 375 Quiz of the Semester" Day?

Section 8.2

PRINCIPLES OF CRYPTOGRAPHY

In symmetric key cryptography, Alice and Bob share a secret key, K_S.



Symmetric key crypto has evolved to increase randomness of tables/functions.

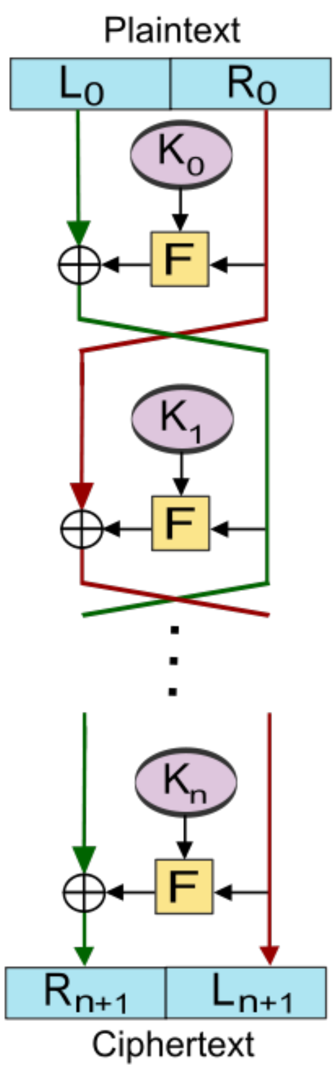
- **Ancient**: Monoalphabetic Cipher
- **Enlightenment**: Polyalphabetic Cipher
- **Modern**: Stream & Block Ciphers

Shannon* described two important properties of good cryptography.

- **Confusion**: Each ciphertext character should depend on several parts of the key.
- **Diffusion**: Frequency statistics of input are diffused over several characters of ciphertext.

* *Claude Shannon: "Communication theory of secrecy systems." 1949.*

DES is a block-cipher that uses a 56-bit key with 16 permutation rounds.

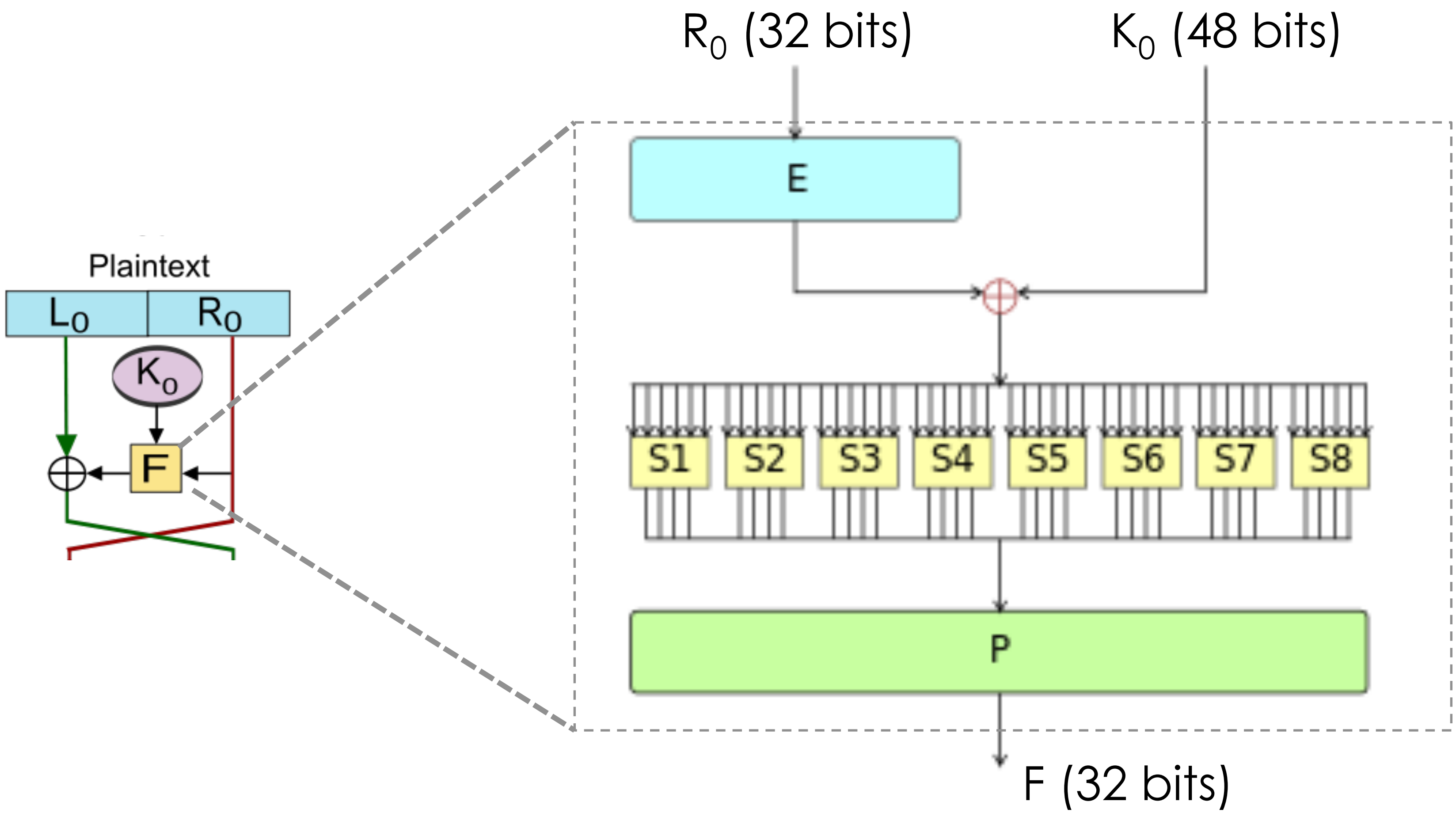


L_i, R_i: Left and right half of block

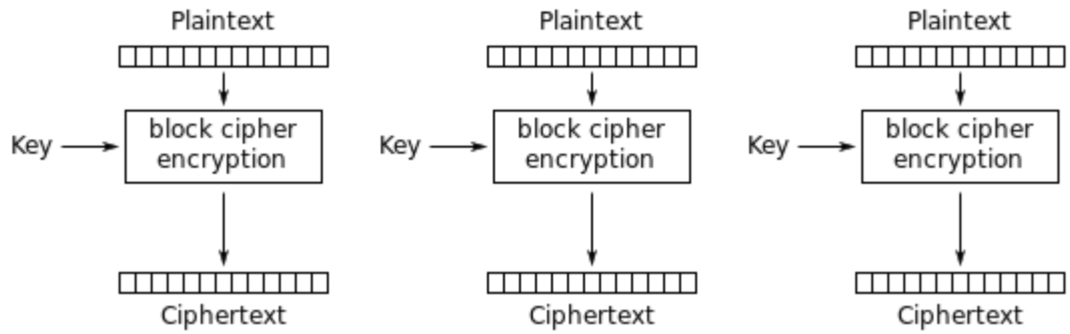
K_0, K_1, …, K_n: Subkeys generated from full key

F: Feistel Cipher

The Feistel Cipher uses expansion and permutation to ensure confusion and diffusion.

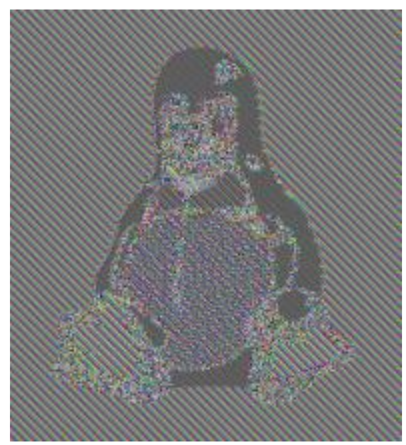


Care needs to be taken in how to apply block ciphers.



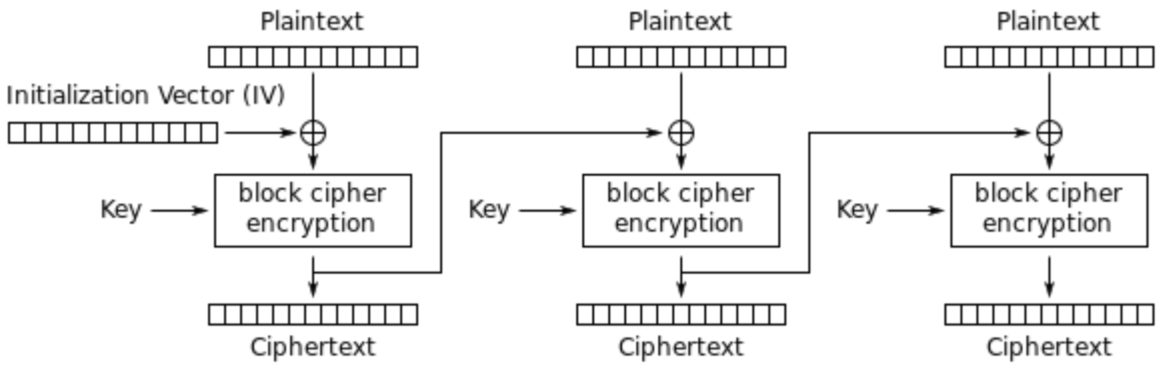
Electronic Codebook (ECB) mode encryption

Original



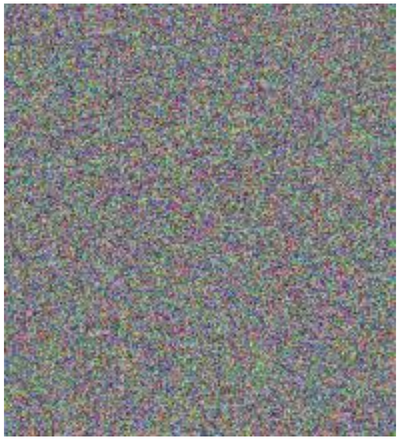
Encrypted in ECB mode

Cipher Block Chaining (CBC) introduces additional randomness into encryption.



Cipher Block Chaining (CBC) mode encryption

Original



Encrypted in CBC mode

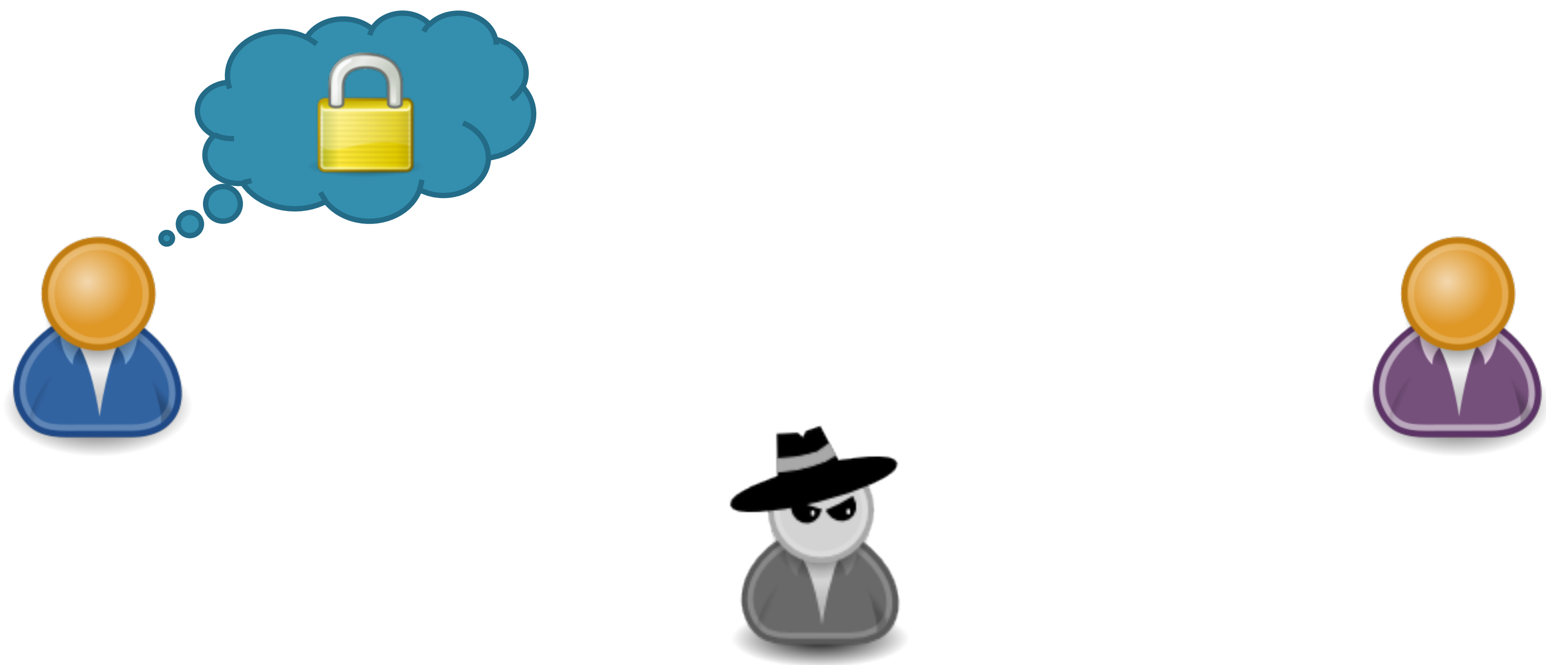
How would you give a new shared, private key to a friend in Maine?

A.	E-mail it to them.
B.	Encrypt it, then email it to them.
C.	Put it on a USB drive and send that to them via the USPS.
D.	Put it on a USB drive, then give it to them in person.
E.	Some other way.

Suppose you want to ship a package to someone else.

We'll assume it won't be stolen… but it might be read.

"I bet we can use locks for this!"



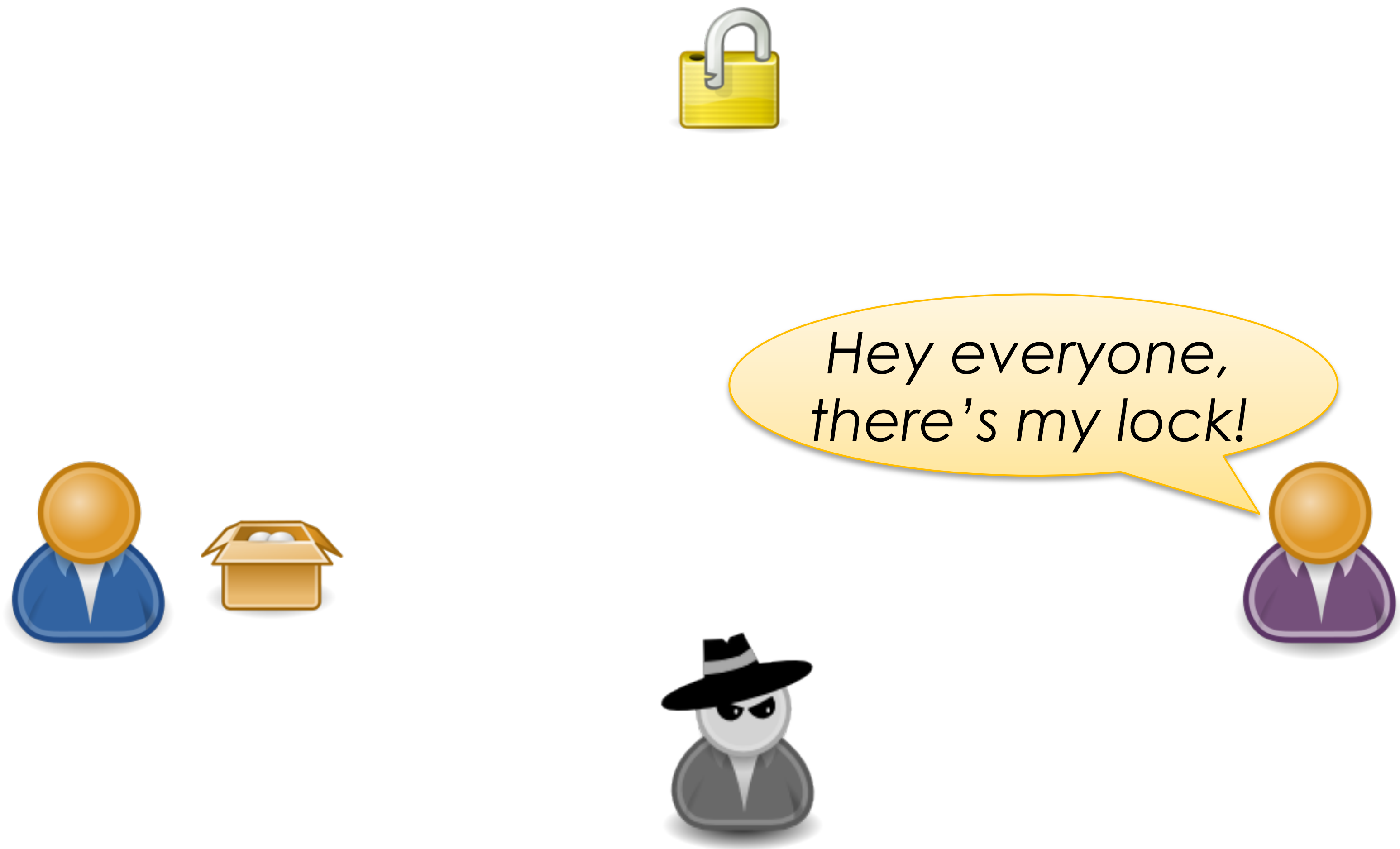
First, we'll add our lock to the box.

Next, we send it to the other person, who applies their own lock.

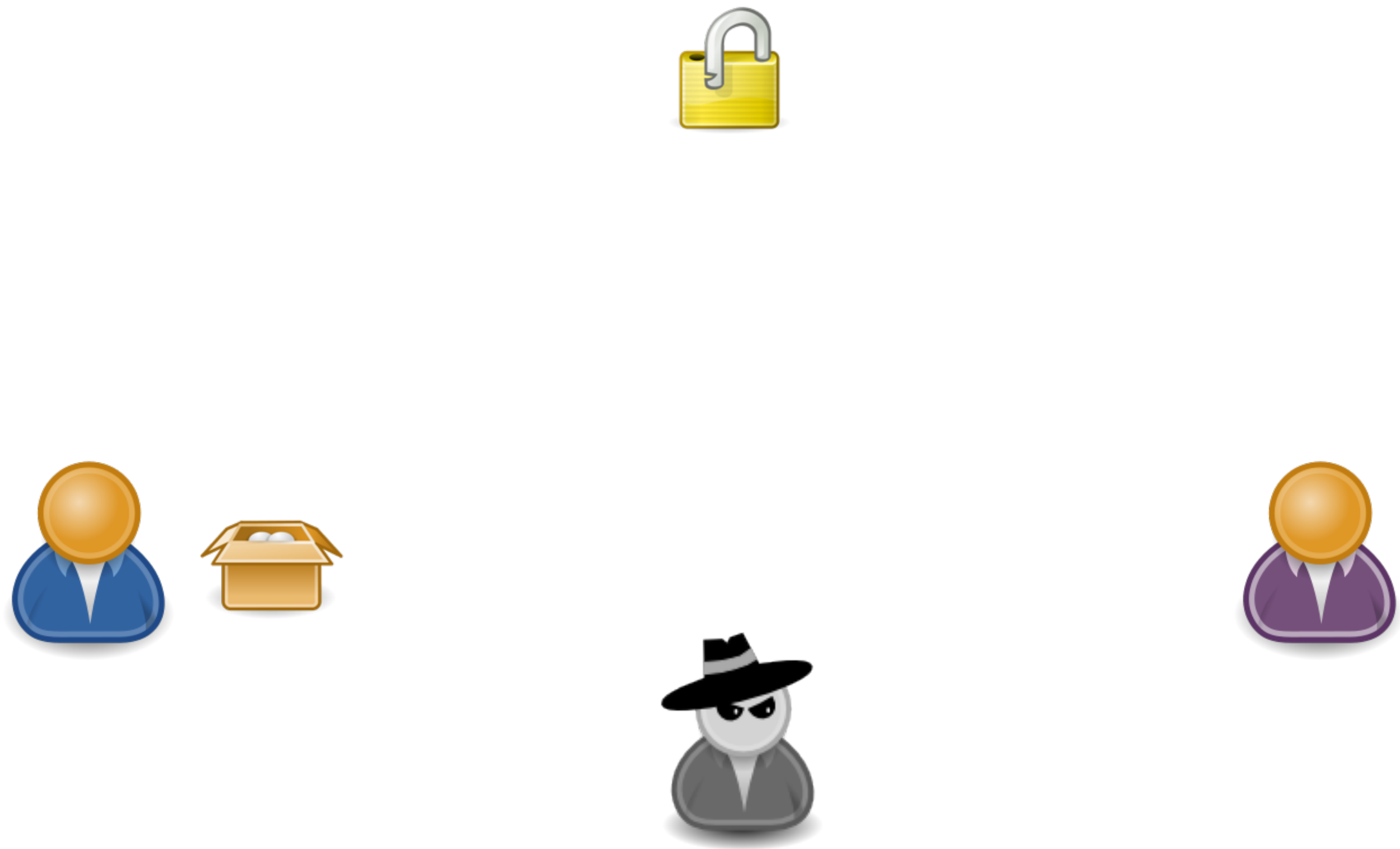
We can remove our lock now, leaving a single lock on the box.

Finally, the recipient can remove their lock and view the contents.

We only really need one private key.

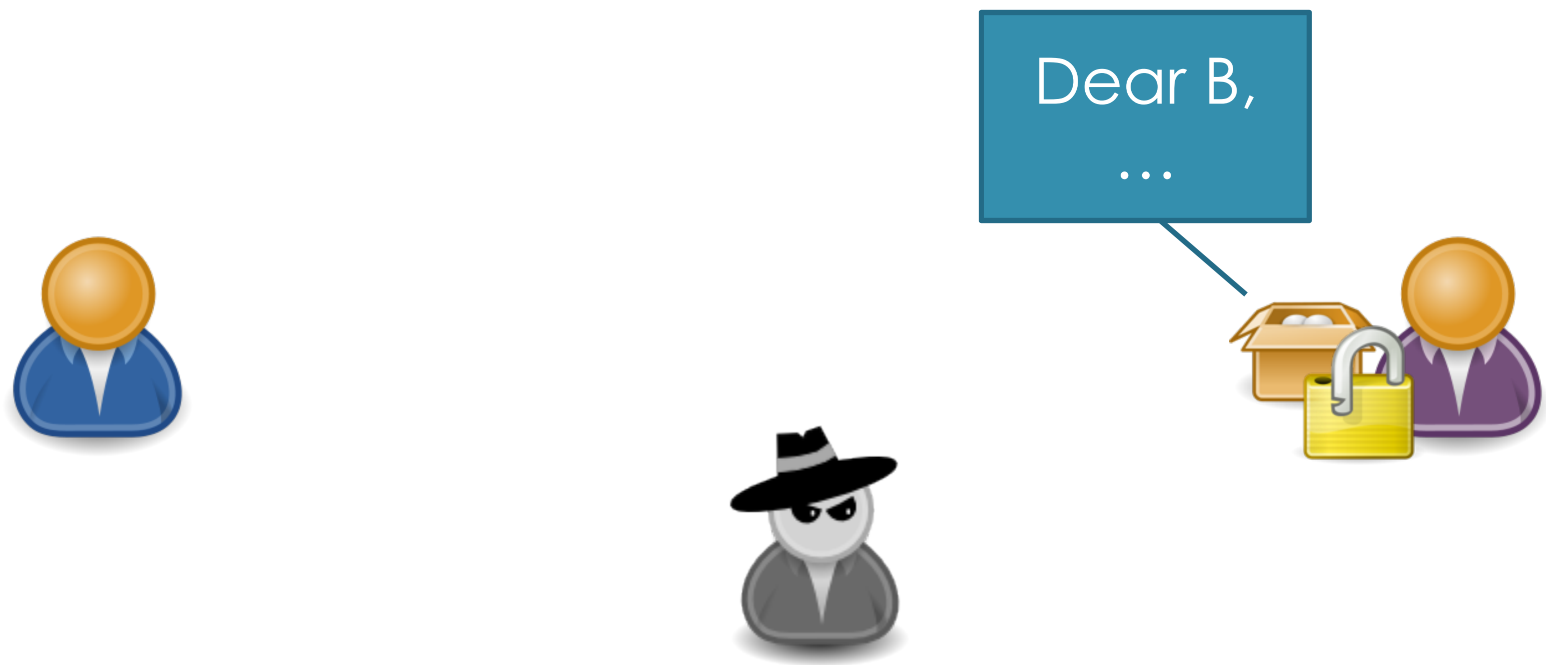


We can take the publicly available open lock and apply it.



We can take the publicly available open lock and apply it.

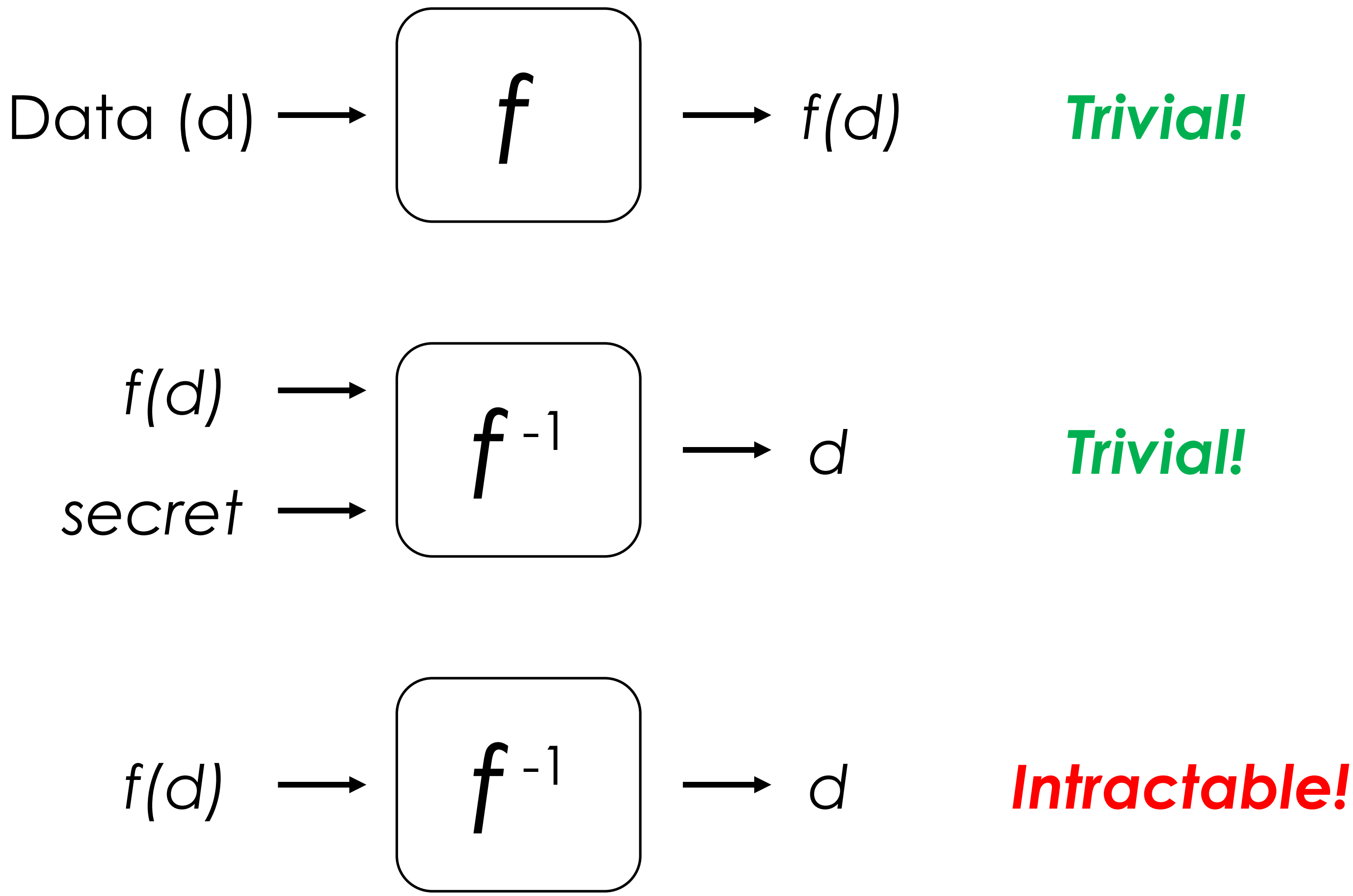
The recipient can use their private key to unlock the box.



Section 8.2.2

PUBLIC KEY ENCRYPTION

We need to find a function (f) that is easy to apply but generally difficult to reverse.



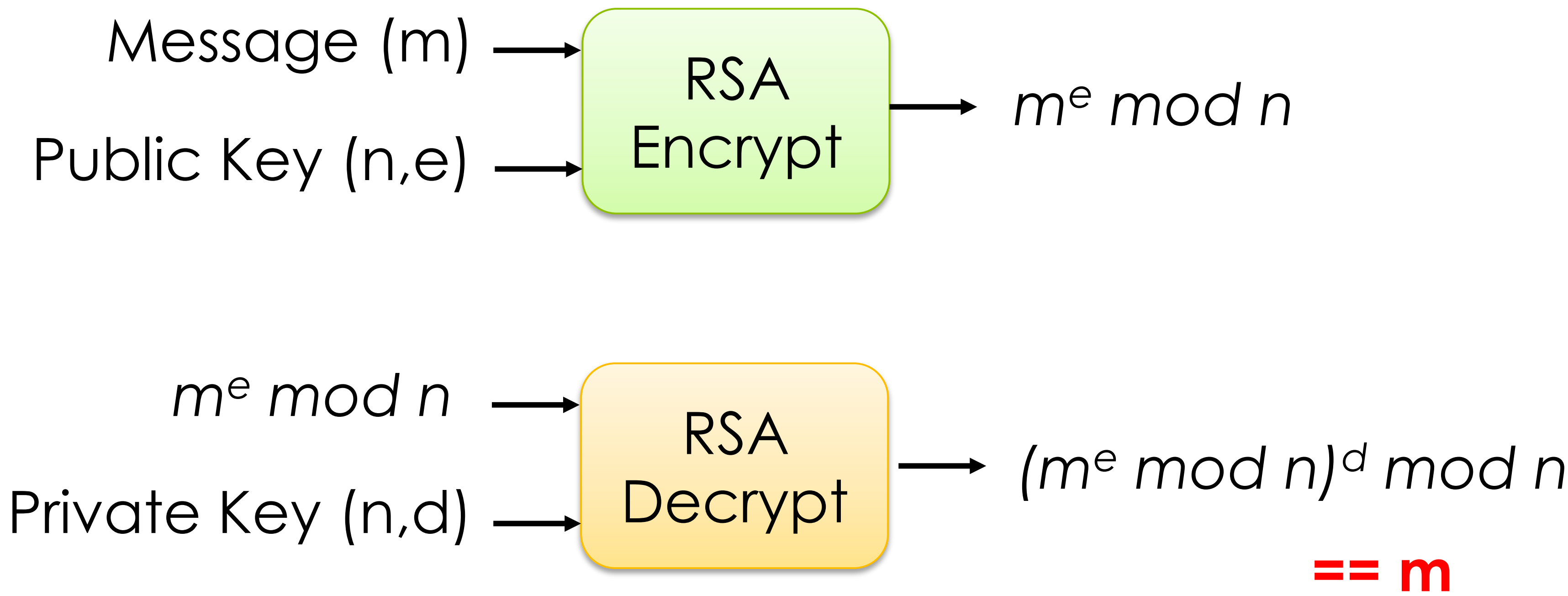
RSA relies on the difficulty in factoring prime numbers to generate keys.

1. Pick 2 large prime numbers, p and q
2. Compute:
   - $n = p*q$
   - $z = (p-1)*(q-1)$
3. Pick e such that:
   - $e < n$
   - e and z are relatively prime
4. Pick d such that: $ed \bmod z = 1$

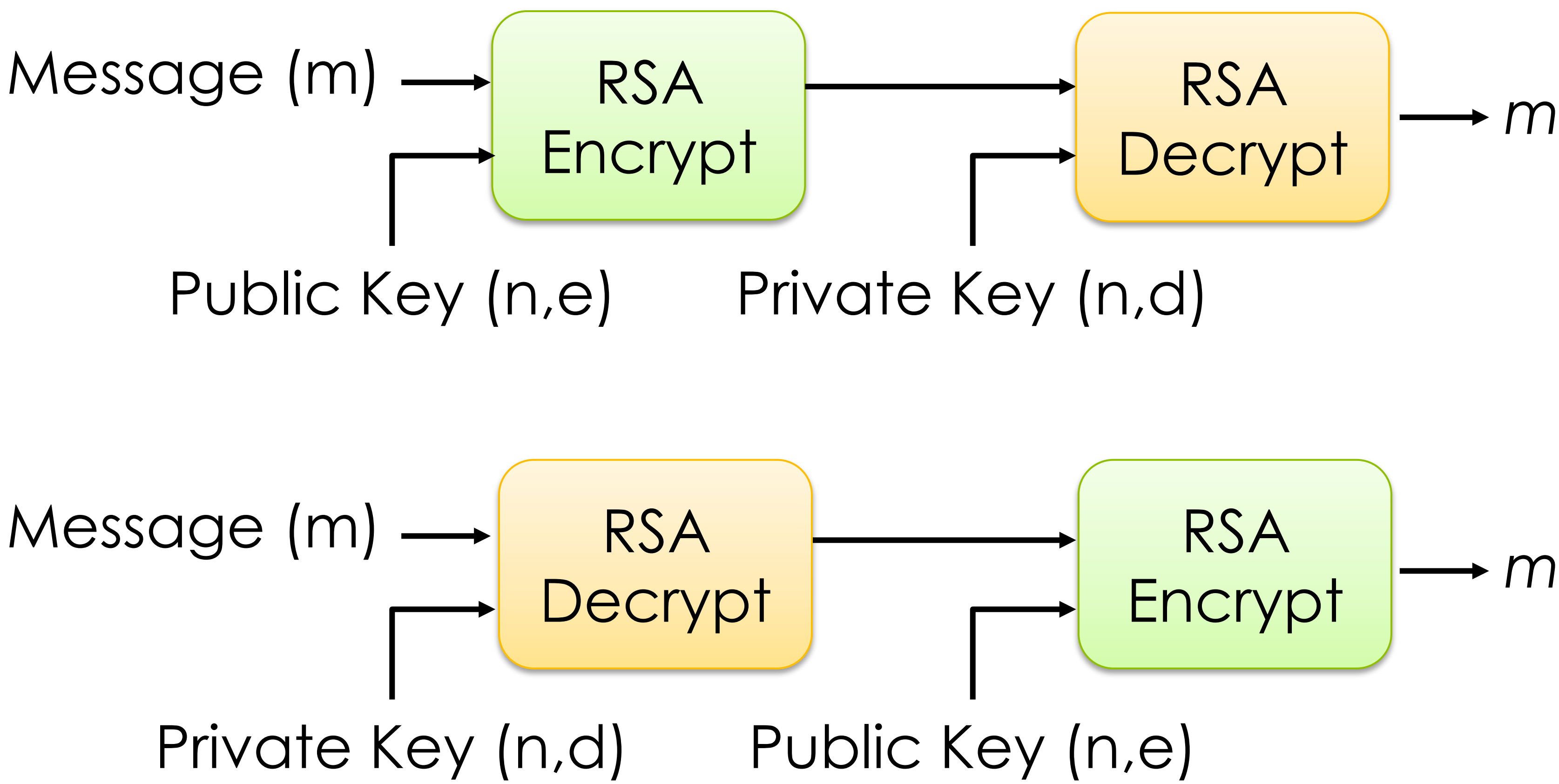
Public Key: (n, e)

Private Key: (n, d)

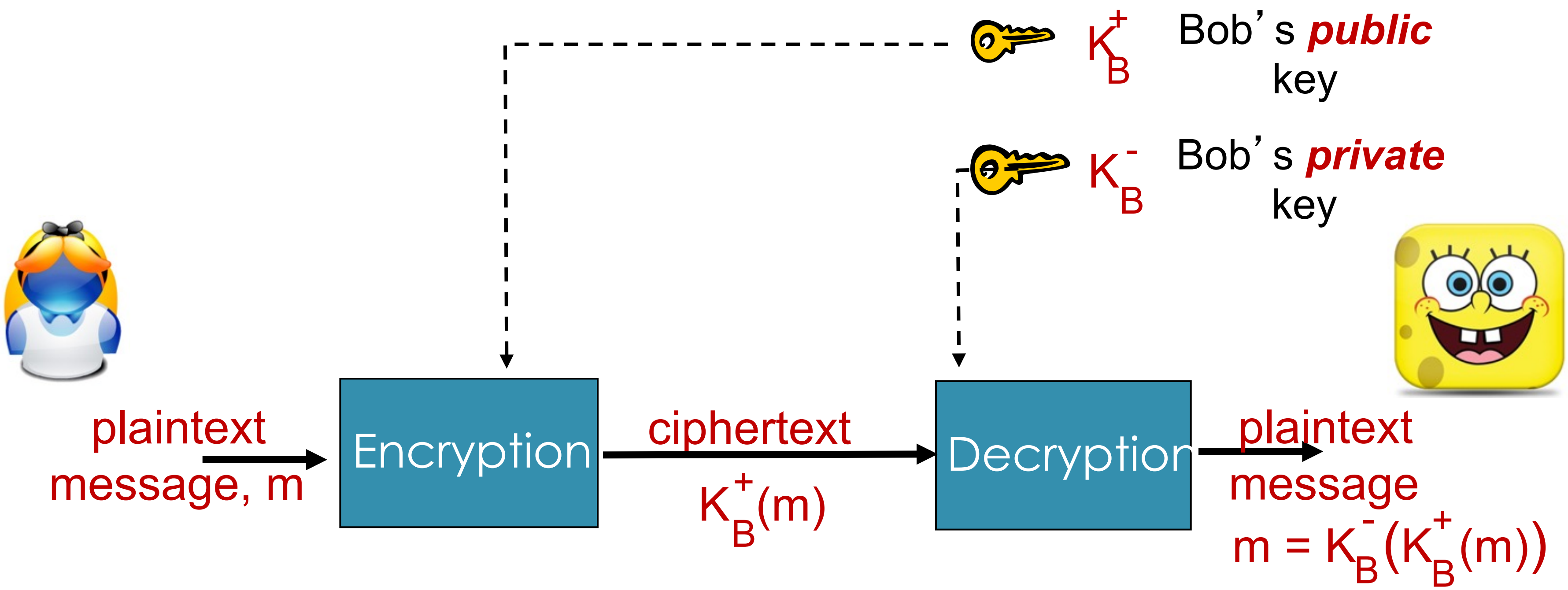
RSA uses modular arithmetic to encrypt and decrypt messages.



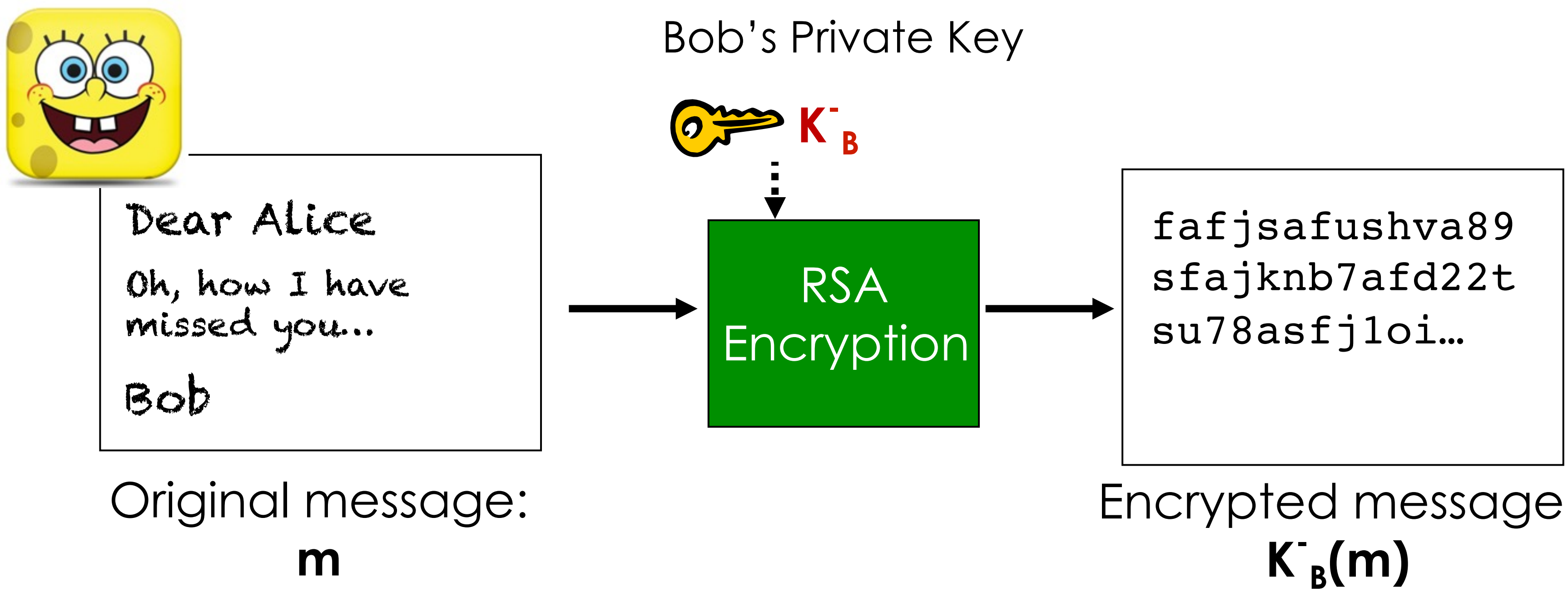
RSA has the important property that it doesn't matter if you "encrypt" or "decrypt" first.



Like symmetric key crypto, public key crypto enables confidentiality.



What does the following setup provide to us?



A.	Confidentiality
B.	Digital Signature
C.	Both A and B
D.	Neither A nor B