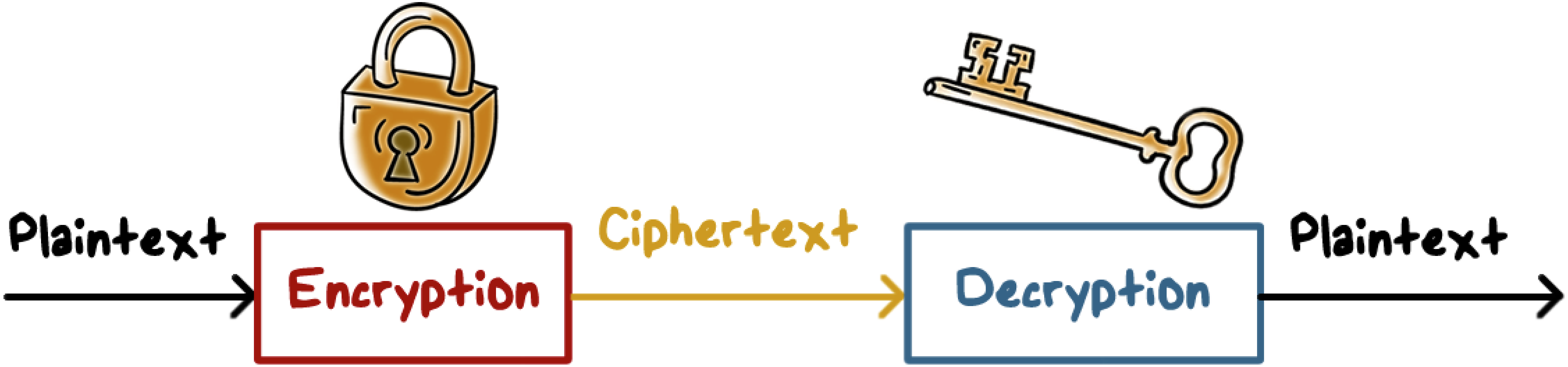
# Intro to Cryptography
## Lesson Introduction

- Basics of encryption and cryptanalysis
- Historical/simple schemes
- Types of cryptography and how they are used for security

# Encryption/Decryption



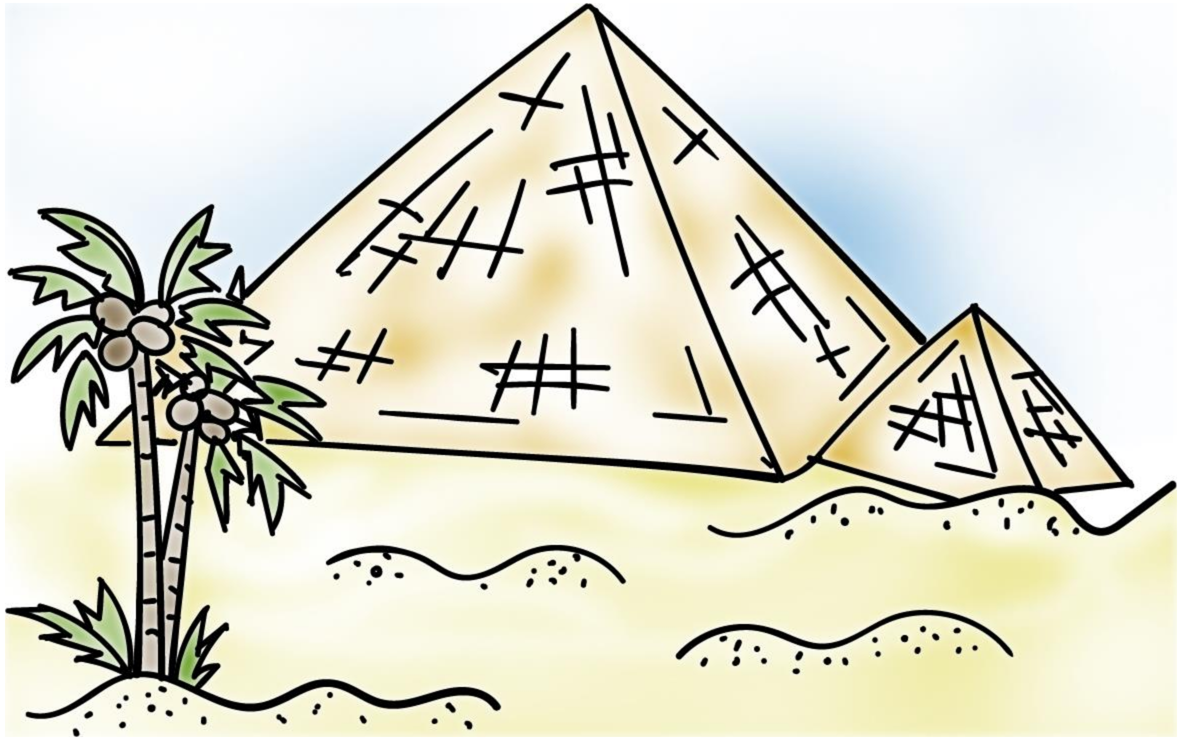

- There is a **one-to-one mapping**
- Provides **confidentiality protection**

# Encryption/Decryption

## Other services:

- **Integrity checking:**
  no tampering
- **Authenticity:**
  verified authorship
- **Authentication:**
  not an imposter

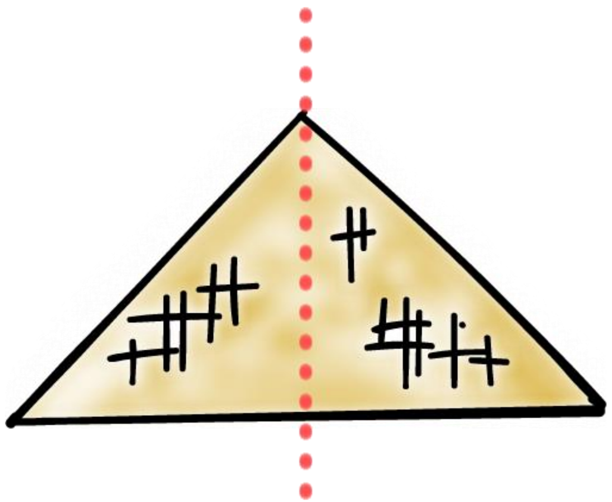
# Encryption Basics

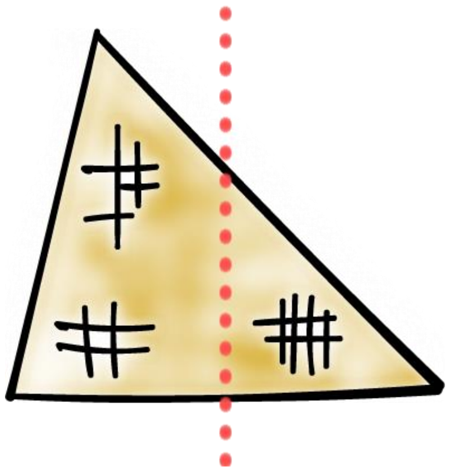


**Ancient crypto:**

- Early signs of encryption in Egypt in ~2000 B.C.
- **Letter-based scheme** (e.g., Caesar’s cipher) ever since

# Encryption Basics

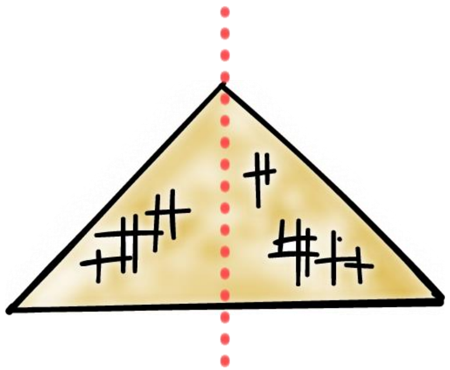




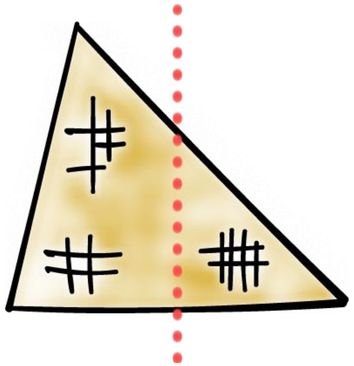
- **Symmetric ciphers:**
  - From ancient time to the presence
- **Asymmetric ciphers**
  - First by Diffie-Hellman-Merkle in 1976

# Encryption Basics

- **Hybrid schemes -** most protocols now use both:



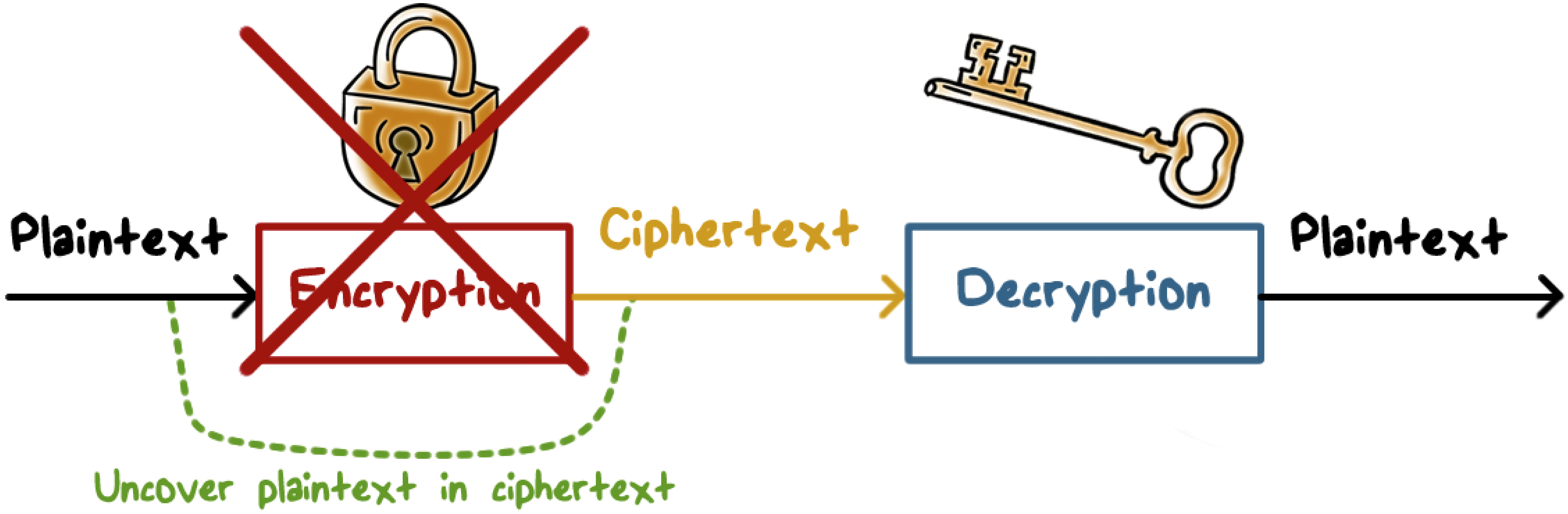
- **Asymmetric ciphers** for authentication, key exchange, and digital signatures



- **Symmetric ciphers** for encryption of data/traffic

# Attacks on Encryption

- **Break a cipher:**
  - **Uncovering** plaintext $p$ from ciphertext $c$, or, alternatively, **discovering** the key



# Attacks on Encryption

- **Brute-force attack**
  - E.g., try all possible keys
- **Cryptanalysis**
  - Analysis of the algorithm and data characteristics
- **Implementation attacks**
  - E.g., side channel analysis
- **Social-engineering attacks**

# Encryption Attack Quiz

If the only form of attack that could be made on an encryption algorithm is **brute- force**, then the **way to counter such attacks** would be to...

- ○ use a longer key length
- ○ use a shorter key length
- ○ use a more complex algorithm
- ○ use a harder to guess key

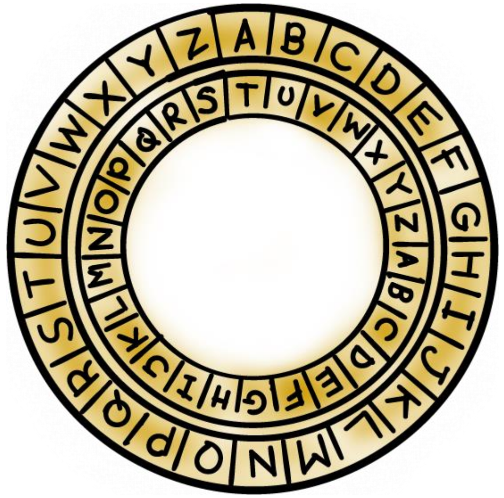
# Simple Ciphers Quiz

Use Caesar's cipher to decode the message:

**LQIRUPDWLRQ VHFXULWB**

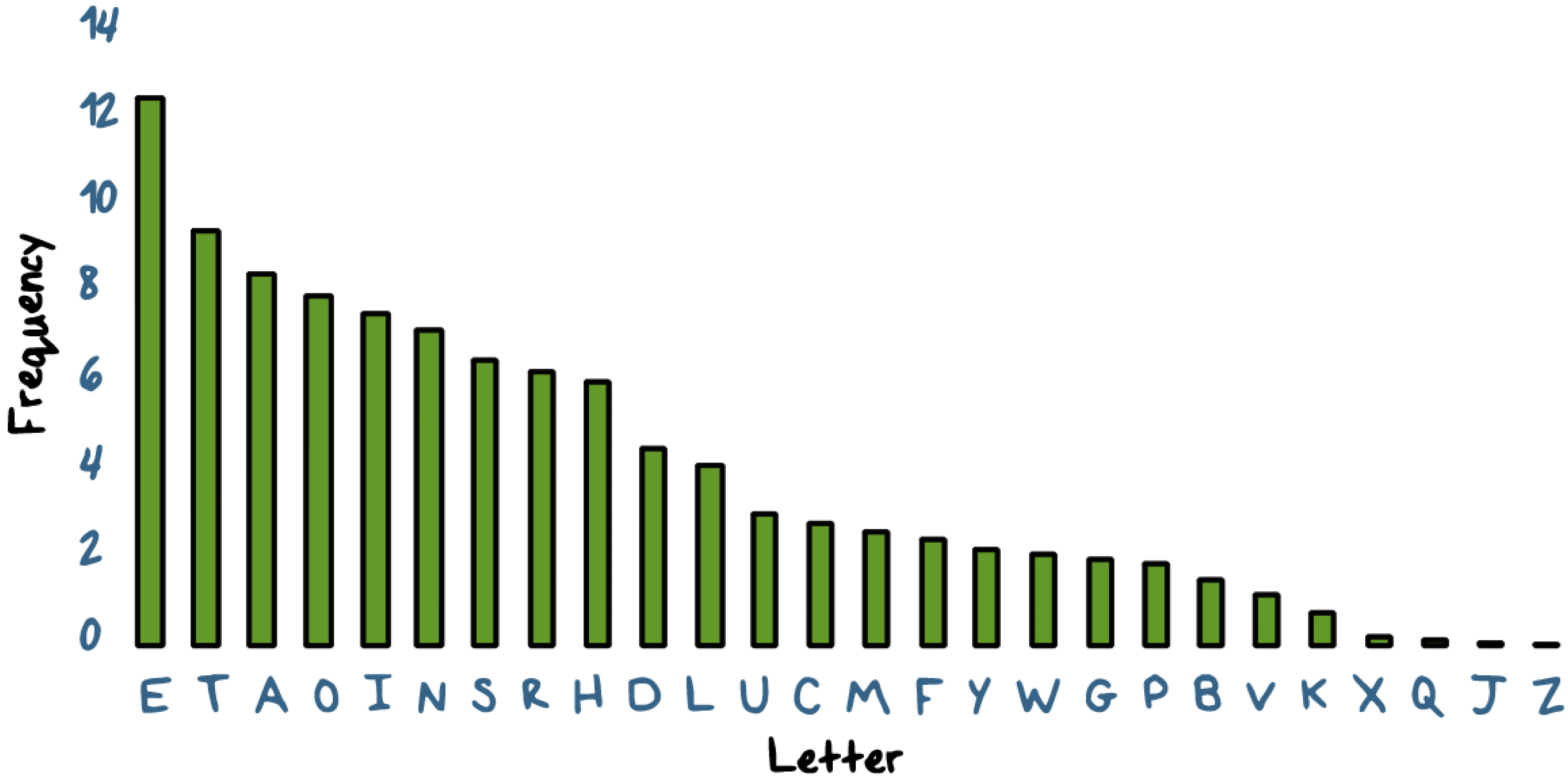
Enter your answer in the text box:

# Simple Ciphers

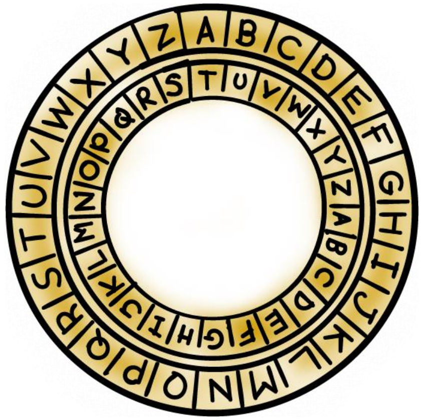


- **Caesar's cipher (or, shift cipher):**
  - E.g., A → D, B → E
  - That is, shift by an offset *n*:
    - (letter + *n*) mod 26
  - **only 26 possible ways** of secret coding
- **Monoalphabetic cipher (or, substitution cipher):**
  - **generalization**, arbitrary mapping of one letter to another
  - 26!, ~4 × $10^{26}$ or ~$2^{88}$
  - Attack with statistical analysis of letter frequencies

# Letter Frequency of Ciphers



# Letter Frequency of Ciphers



- What is plaintext for:

**IQ IFCC VQQR FB RDQ VFLLCQ NA RDQ CFJWHWZ HR BNNB HCC HWWHBSQVQBRE HWQ VHLQ**

**WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL ARRANGEMENTS ARE MADE**

- In practice, also consider frequency of letter pairs, triples

# Monoalphabetic Cipher Quiz

Try to decipher this method using the Monoalphabetic Cipher:

**WAIT IT WAS SAD**

Enter your answer in the text box:

# Vigenere Cipher

- Plaintext:

  ATTACKATDAWN

- Key:

  LEMON

- Keystream:

  LEMONLEMONLE

- Ciphertext:

  LXFOPVEFRNHR

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

# Vigenere Cipher Quiz

What **weaknesses** can be exploited in the Vigenere Cipher?

- [ ] It uses a repeating key letters
- [ ] It requires security for the key, not the message
- [ ] The length of the key can be determined using frequency

# What should be Kept Secret?

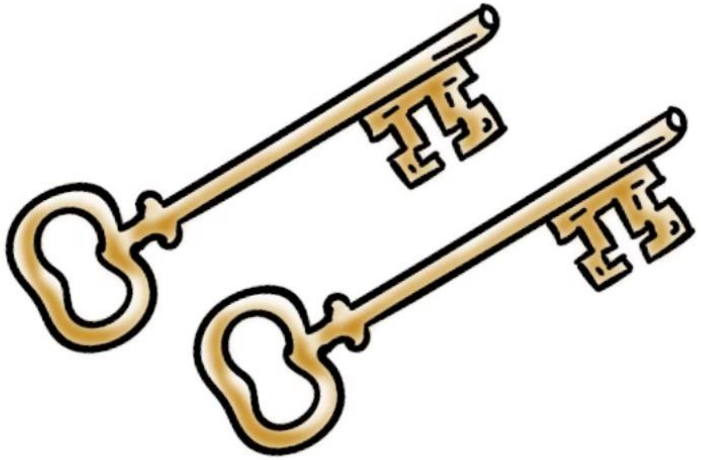

- **Kerckhoff's principle:**
  - A **cryptosystem** should be secure even if the attacker knows all details about the system, with exception of the secret key

- **In practice:**
  - Only use **widely known ciphers** that have been crypto analyzed for several years by good cryptographers
    - E.g., established standards

# Types of Cryptography

## Secret key cryptography:

- **one key** same key for encryption and decryption



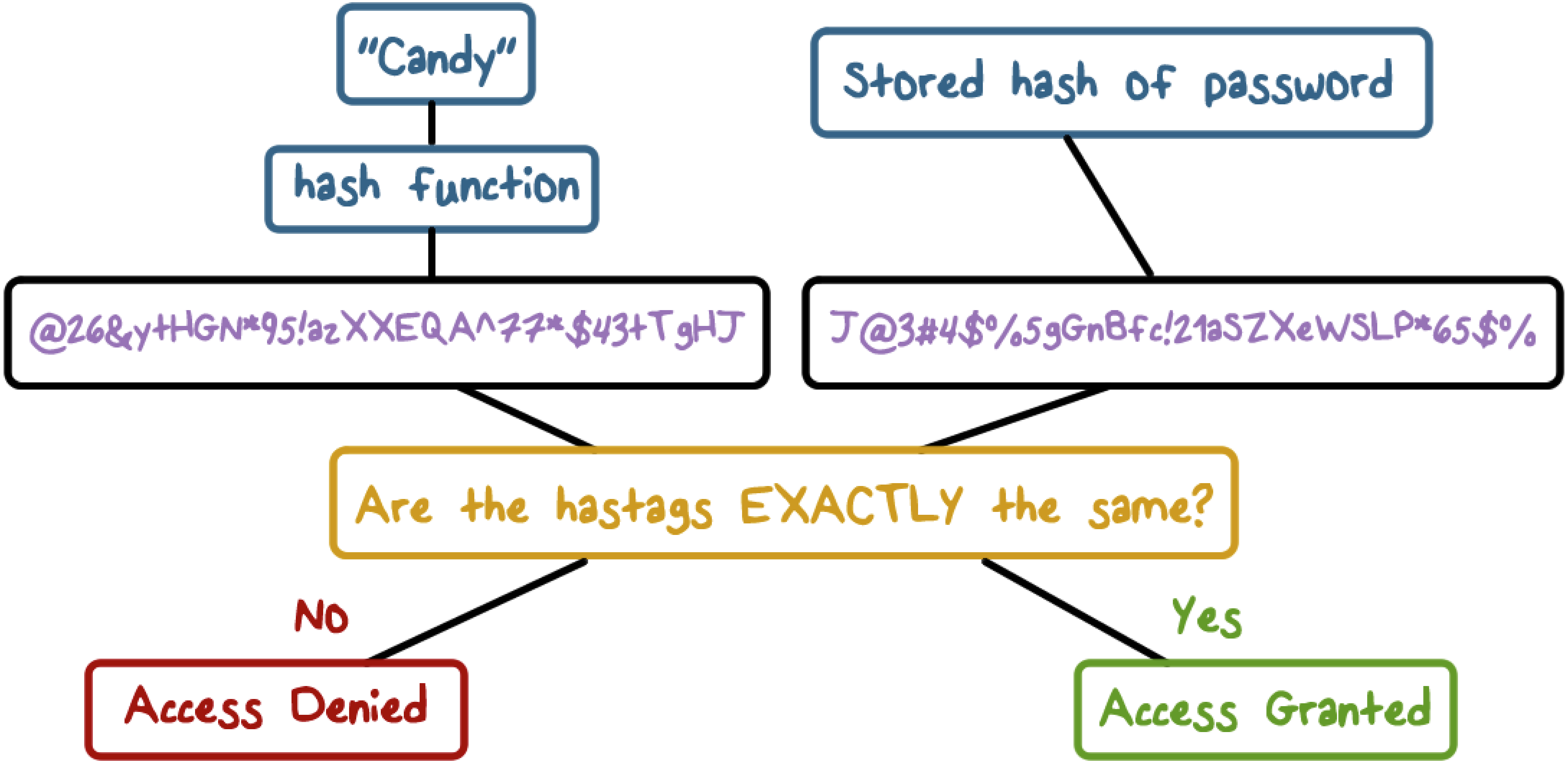
## Public key cryptography:

- **two keys**
  - Public for encryption, private for decryption
  - Private for signing and public for verification

# Hash Functions

- Compute message digest of **data of any size**
- **Fixed length output**: 128-512 bits
- Easy to compute $H(m)$
- Given $H(m)$, no easy way to find $m$
  - ***One-way function***
- Given $m_1$, it is computationally infeasible to find $m_2 \neq m_1$ s.t. $H(m_2) = H(m_1)$
  - **Weak collision resistant**
- Computationally infeasible to find $m_1 \neq m_2$ s.t. $H(m_1) = H(m_2)$
  - **Strong collision resistant**

# Hash Functions for Passwords

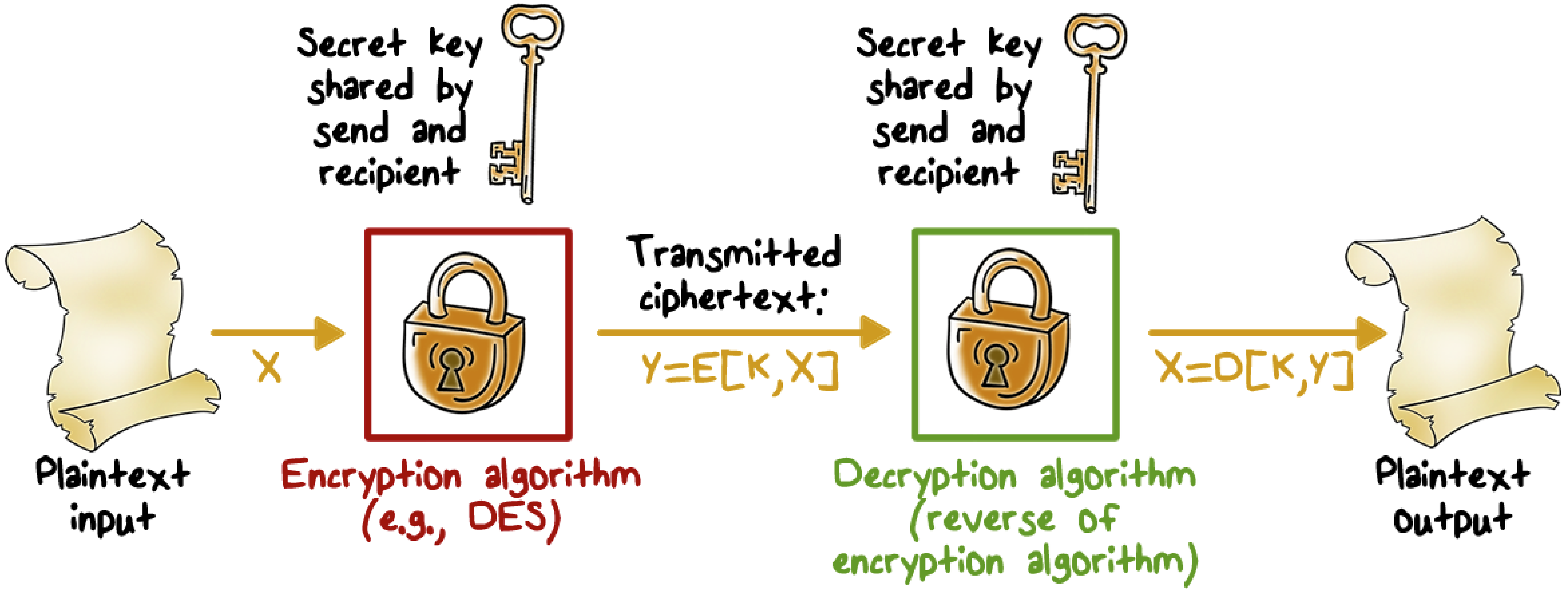


# Hash Function Quiz

Which of the following characteristics would i**mprove password security**?

- [ ] Use a one-way hash function
- [ ] Should not use the avalanche effect
- [ ] Should only check to see that the hash function output is the same as stored output

# Symmetric Encryption



# Comparison of Encryption Algorithms

| | DES | Triple DES | AES |
|---|---|---|---|
| Plaintext block size (bits) | 64 | 64 | 128 |
| Ciphertext block size (bits) | 64 | 64 | 128 |
| Key size (bits) | 56 | 112 or 168 | 128, 192, or 256 |

DES = Data Encryption Standard
AES = Advanced Encryption Standard

# Comparison of Encryption Algorithms

| Key size (bits) | Cipher | Number of Alternative Keys | Time Required at $10^9$ descryptions/s | Time Required at 10 descryptions/s |
|---|---|---|---|---|
| 56 | DES | $2^{56} \approx 7.2 \times 10^{16}$ | $2^{55}$ ns = 1.125 years | 1 hour |
| 128 | AES | $2^{128} \approx 3.4 \times 10^{38}$ | $2^{127}$ ns = $5.3 \times 10^{21}$ years | $5.3 \times 10^{17}$ years |
| 168 | Triple DES | $2^{168} \approx 3.7 \times 10^{50}$ | $2^{167}$ ns = $5.3 \times 10^{33}$ years | $5.8 \times 10^{29}$ years |
| 192 | AES | $2^{192} \approx 6.3 \times 10^{57}$ | $2^{191}$ ns = $5.3 \times 10^{40}$ years | $9.8 \times 10^{36}$ years |
| 256 | AES | $2^{256} \approx 1.2 \times 10^{77}$ | $2^{255}$ ns = $5.3 \times 10^{60}$ years | $1.8 \times 10^{56}$ years |

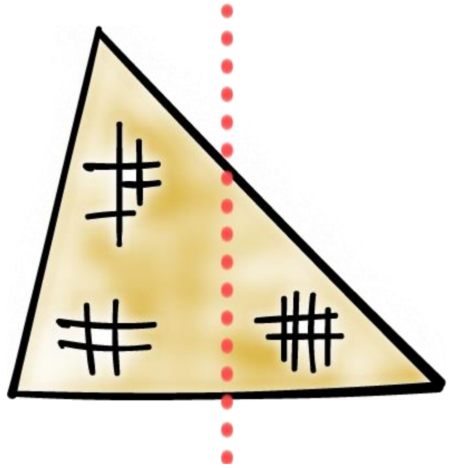
# Symmetric Encryption Quiz

Select the correct definition for **each type of attack**:

A. A method to determine the encryption function by analyzing known phrases and their encryption
B. Analyzing the effect of changes in input on the encrypted output
C. Compare the ciphertexts with its known plaintext
D. A method where a specific known plaintext is compared to its ciphertext

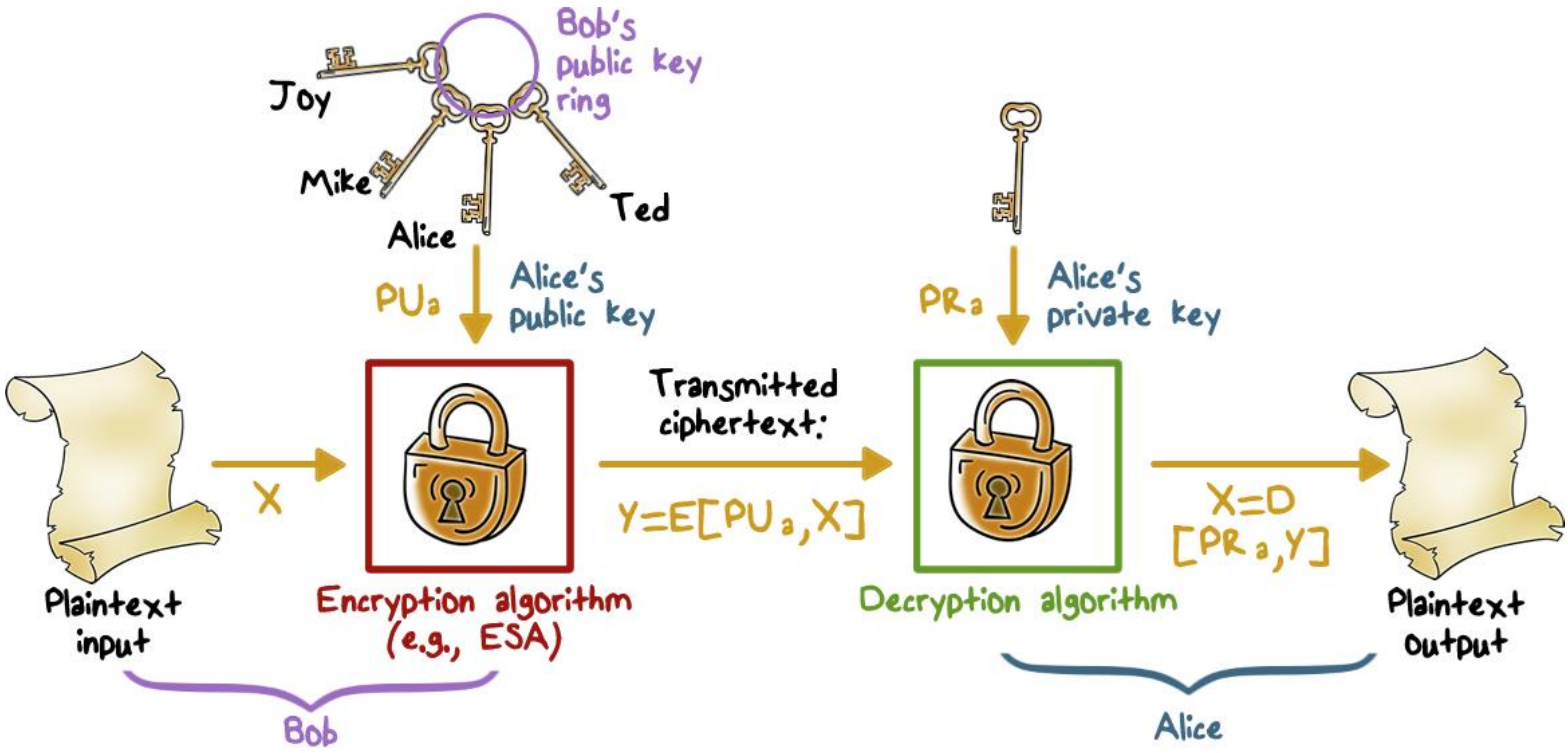
- [ ] known-Plaintext attacks
- [ ] chosen-Plaintext attacks
- [ ] differential cryptanalysis
- [ ] linear cryptanalysis

# Asymmetric Encryption



- **Plaintext**: Readable message or data that is fed into the algorithm
- **Encryption algorithm:** Performs transformations on the plaintext
- **Public and private key:** Pair of keys, one for encryption, one for decryption
- **Ciphertext**: Scrambled message produced as output
- **Decryption key:** Produces the original plaintext

# Asymmetric Encryption

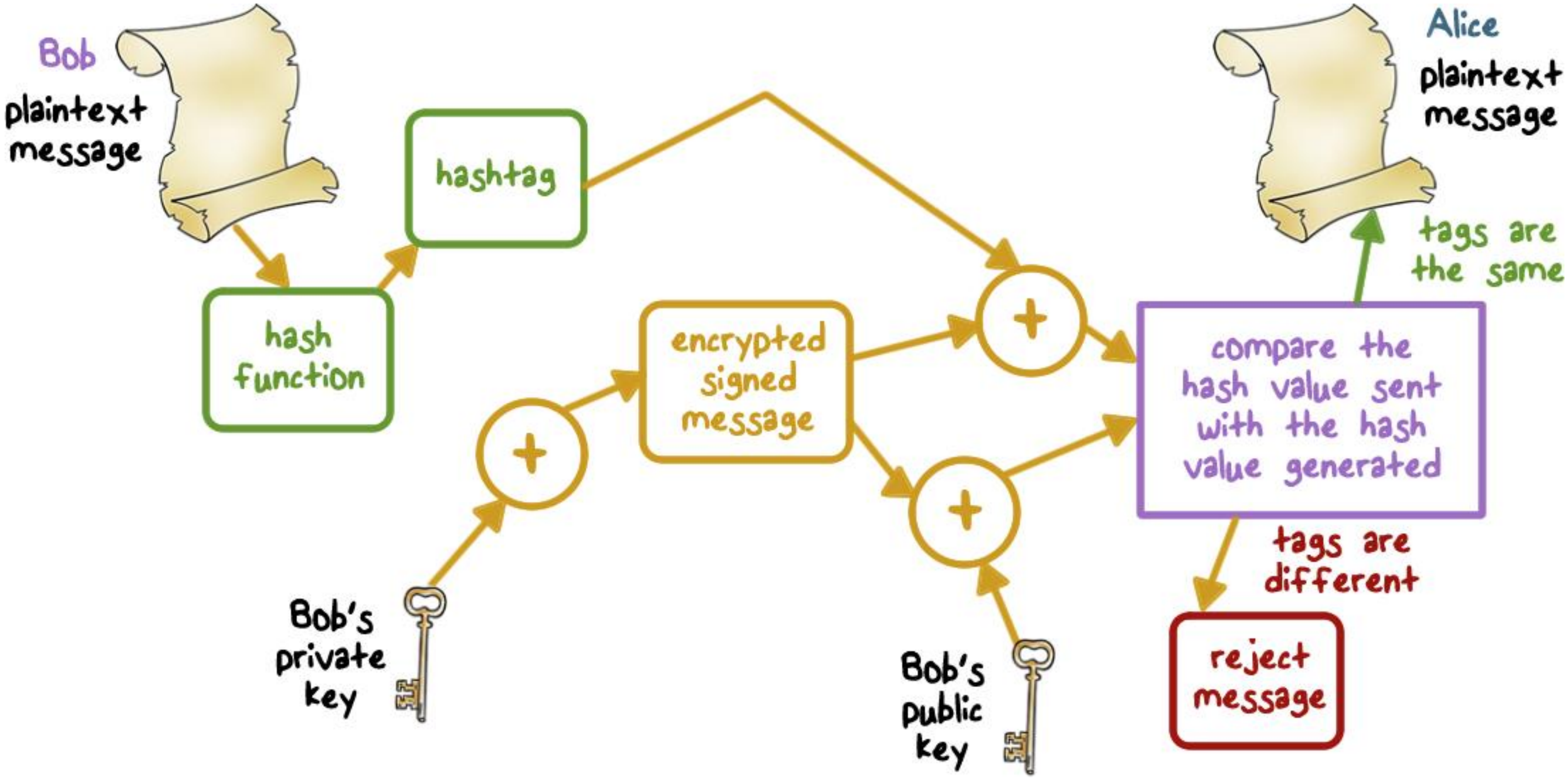


# Asymmetric Encryption Quiz

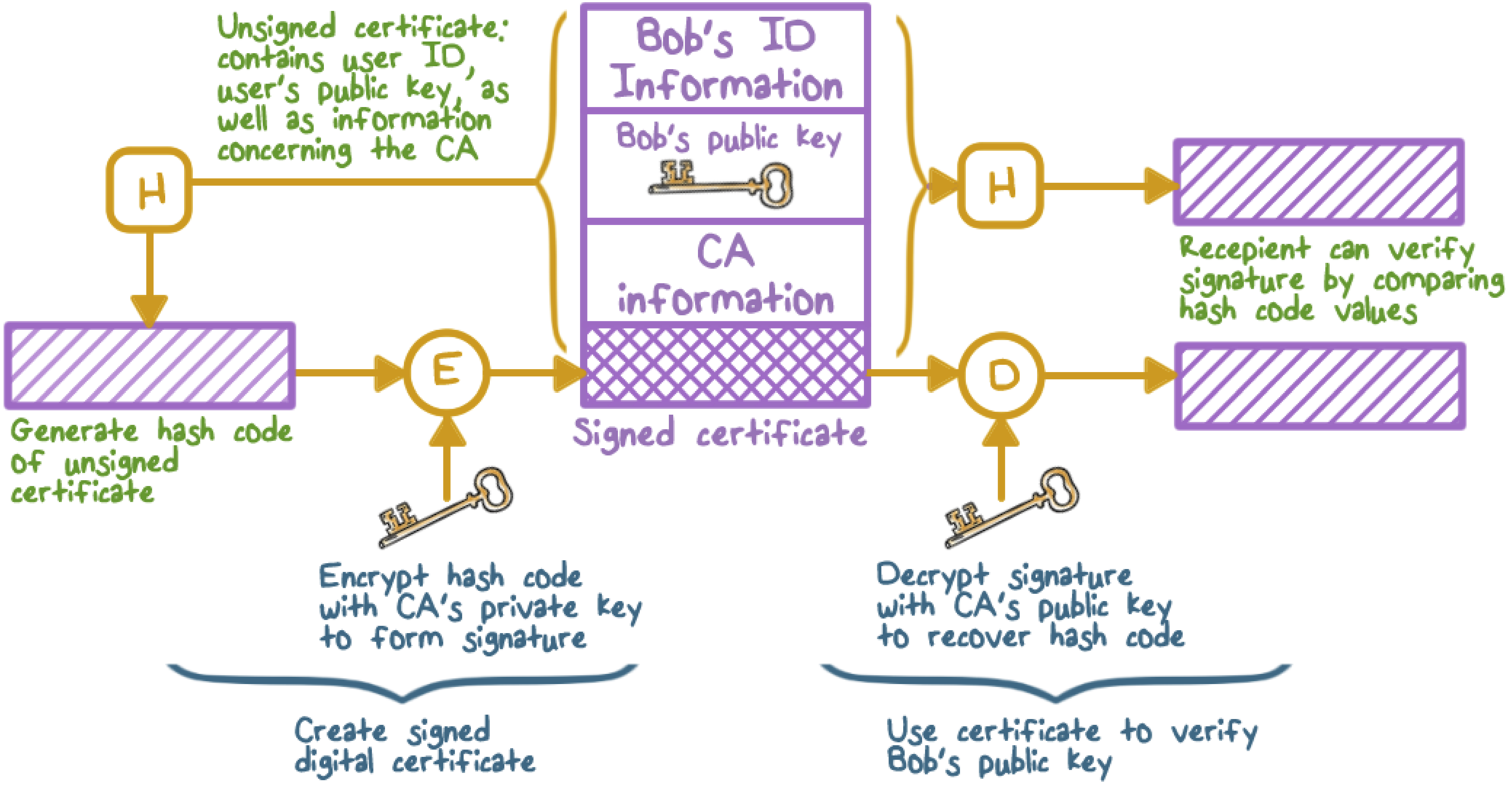
**Check all tasks** for which asymmetric encryption is better:

- [ ] provide confidentiality of a message
- [ ] securely distribute a session key
- [ ] scalability

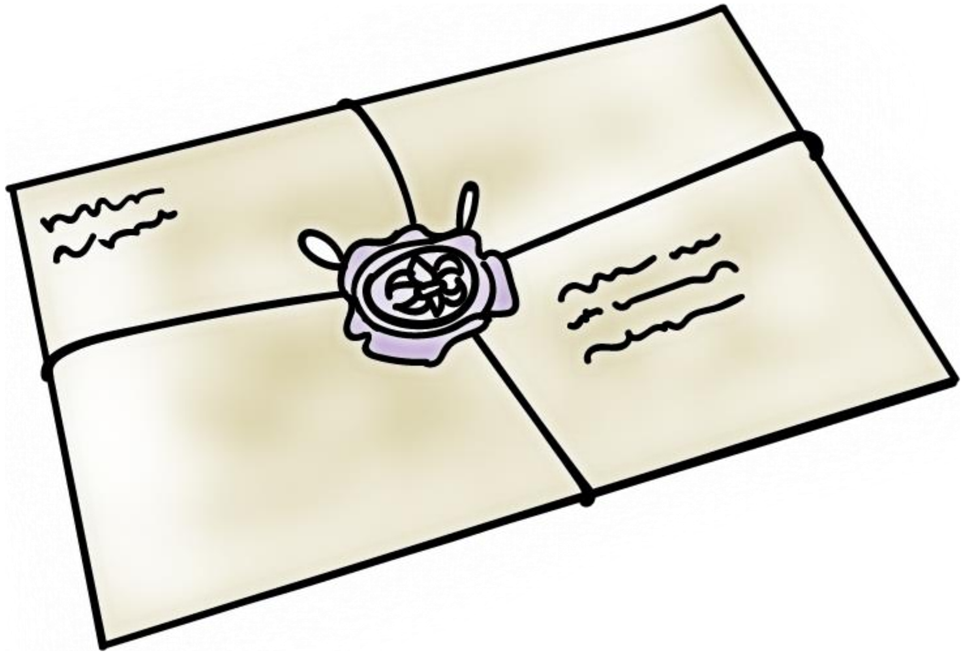
# Digital Signatures



# Digital Signatures

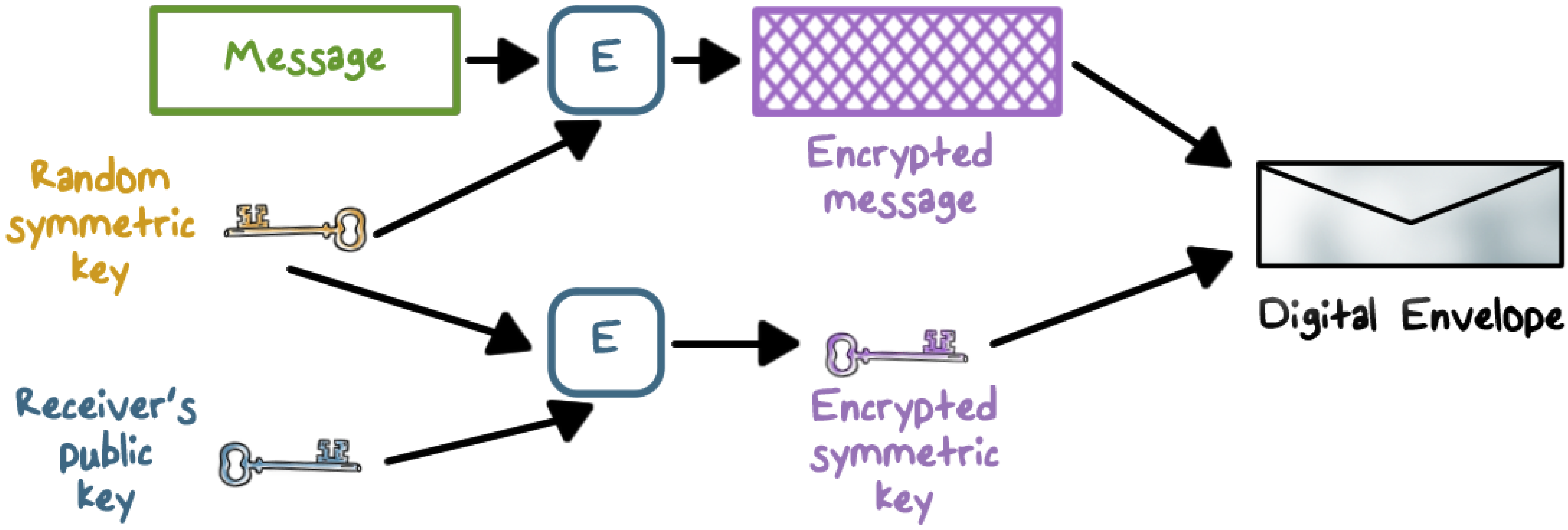


# Digital Envelopes

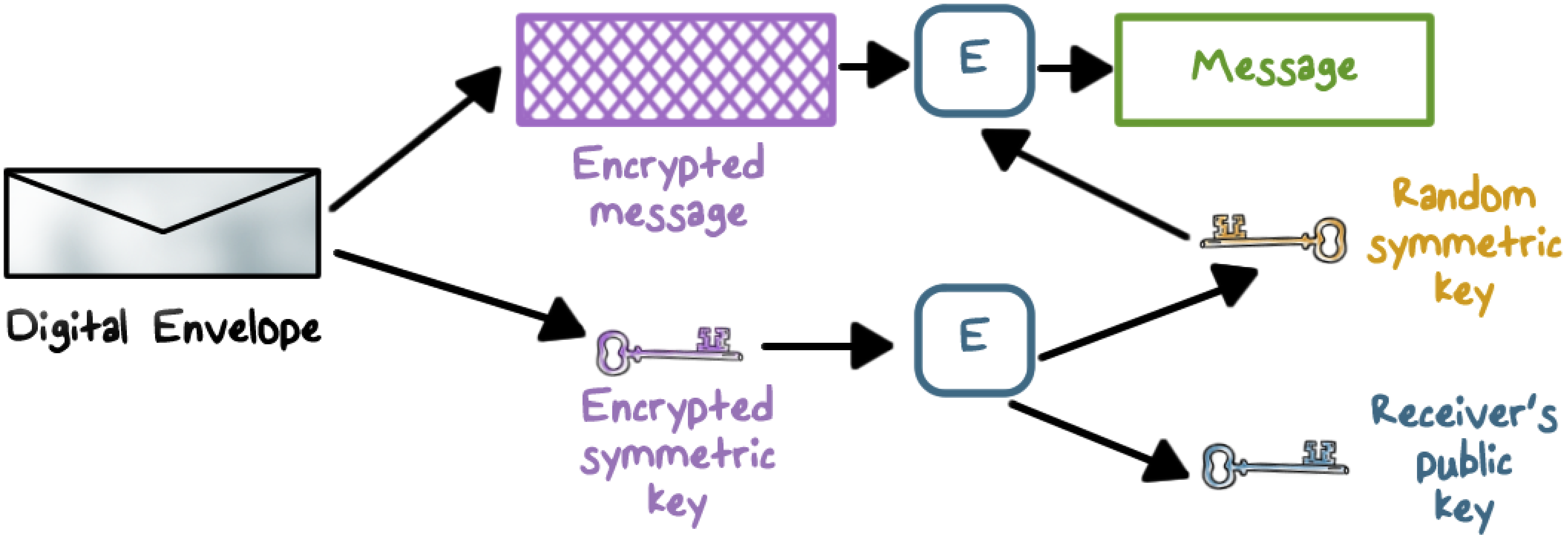


- Protects a message **without needing** to first arrange for sender and receiver to have the same secret key
- Equates to the same thing as a **sealed envelope containing an unsigned letter**

# Digital Envelopes



# Digital Envelopes



# Encryption Quiz

Mark each of the statements either **T for True or F for False**:

- [ ] Symmetric encryption can only be used to provide confidentiality
- [ ] Public-key encryption can be used to create digital signatures
- [ ] Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
- [ ] The secret key is input to the encryption algorithm

# Intro to Cryptography
## Lesson Summary

- Encryption schemes and attacks on encryption have been around for thousands of years.
- Hash: no key, no encryption
- Secret key cryptography: same key for encryption and decryption
- Public key cryptography: public key for encryption and signature verification and private key for decryption and signins