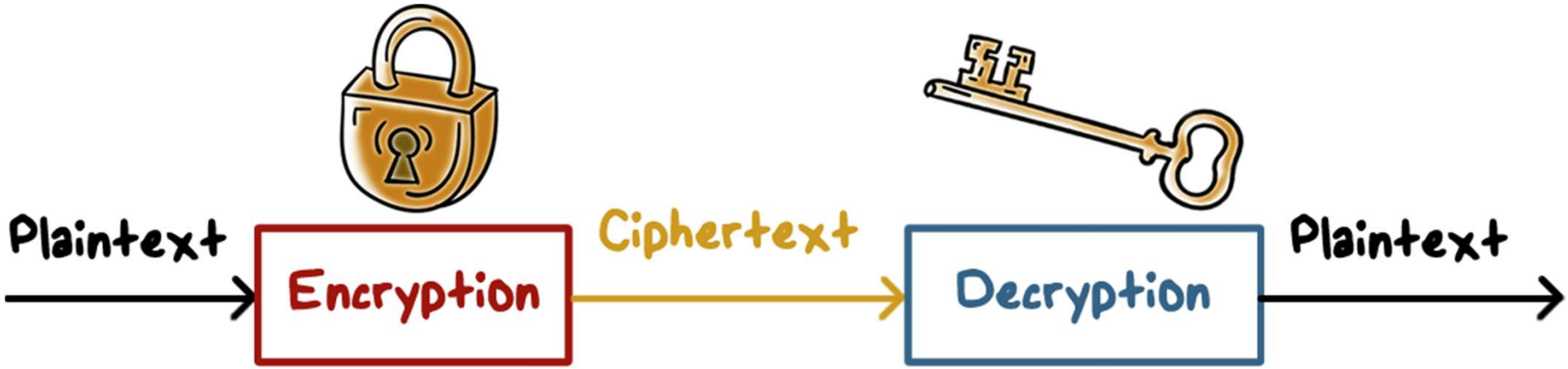
Intro to Cryptography

Lesson Introduction

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

Encryption/Decryption



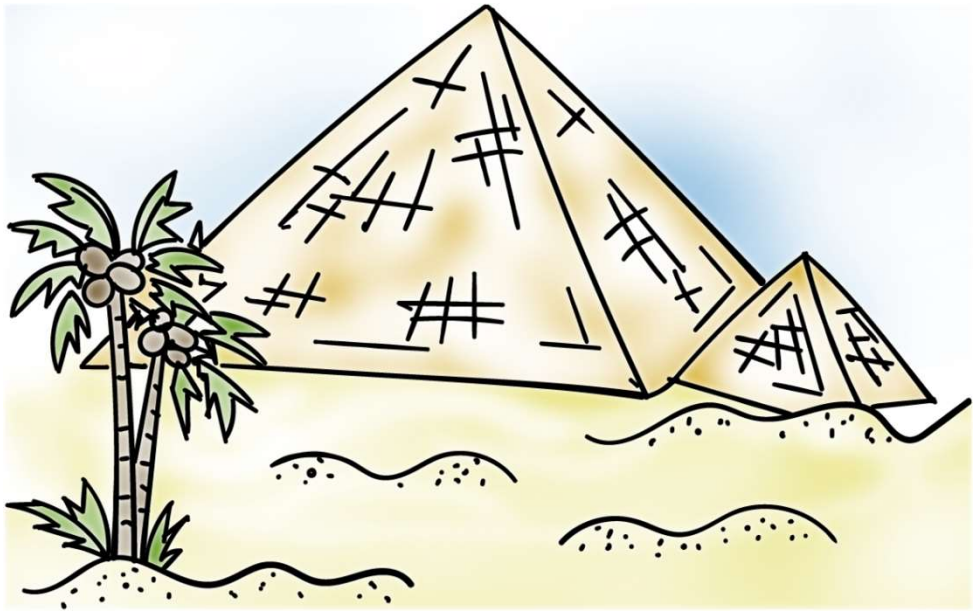
- There is a **one-to-one mapping**
- Provides **confidentiality protection**

Encryption/Decryption

Other services:

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

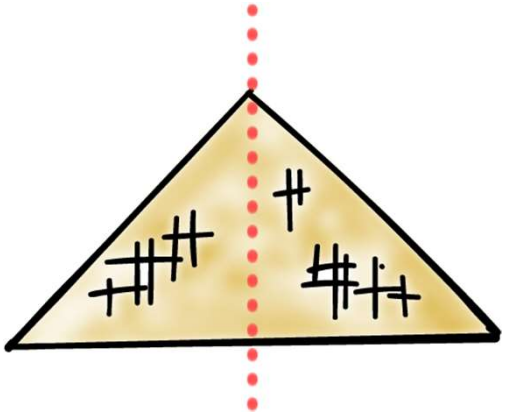
Encryption Basics

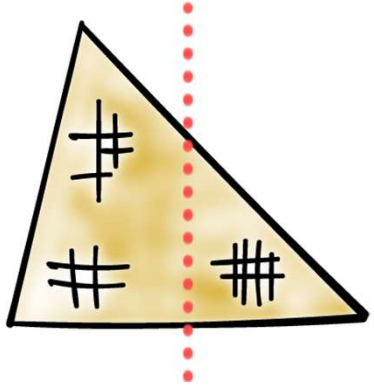


Ancient crypto:

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

Encryption Basics

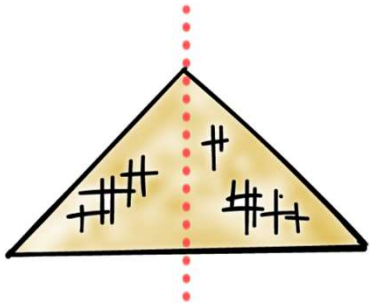




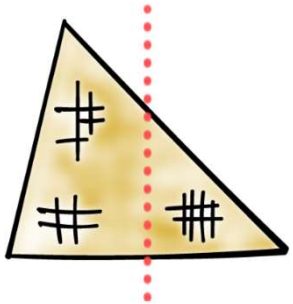
- **Symmetric ciphers:**
  - From ancient time to the presence
- **Asymmetric ciphers**
  - First by Diffie-Hellman-Merkle in 1976

Encryption Basics

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



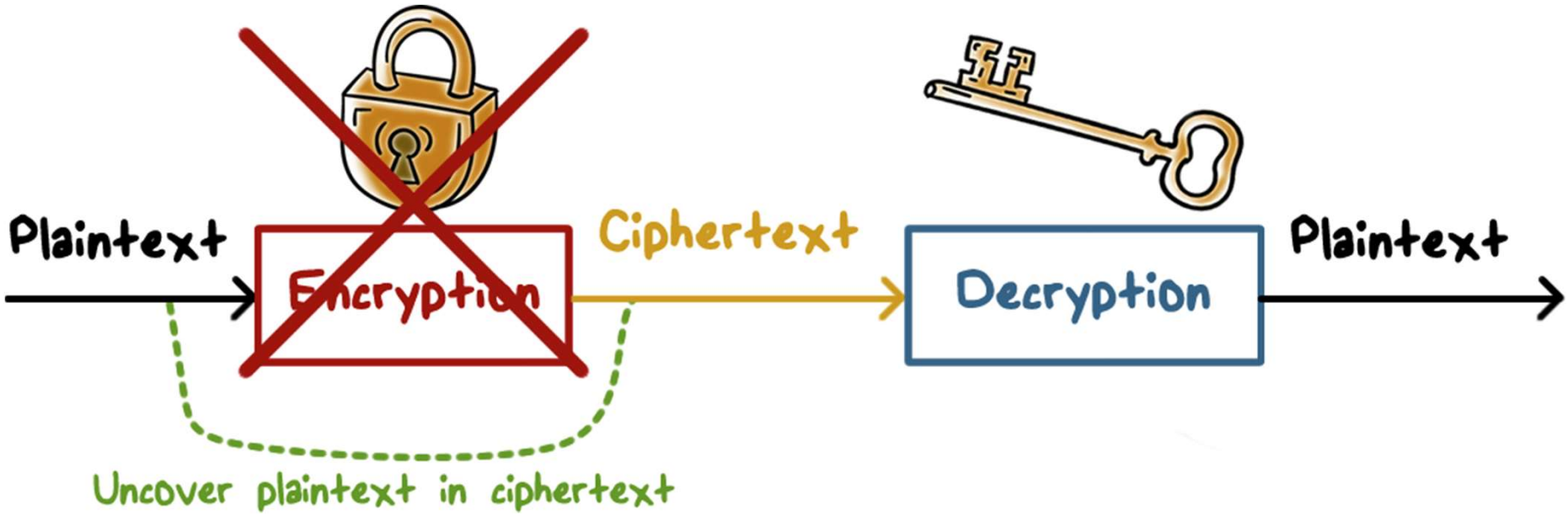
- **Asymmetric ciphers** for authentication, key exchange, and digital signatures



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

Attacks on Encryption

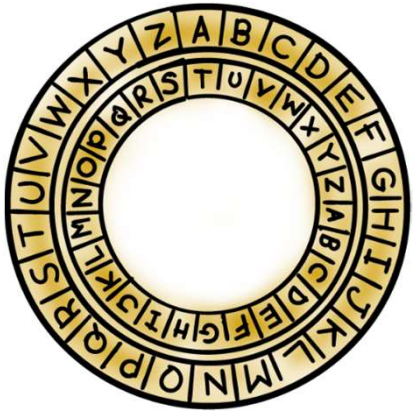
- **Break a cipher:**
  - **Uncovering** plaintext *p* from ciphertext *c*, or, alternatively, **discovering** the key



Attacks on Encryption

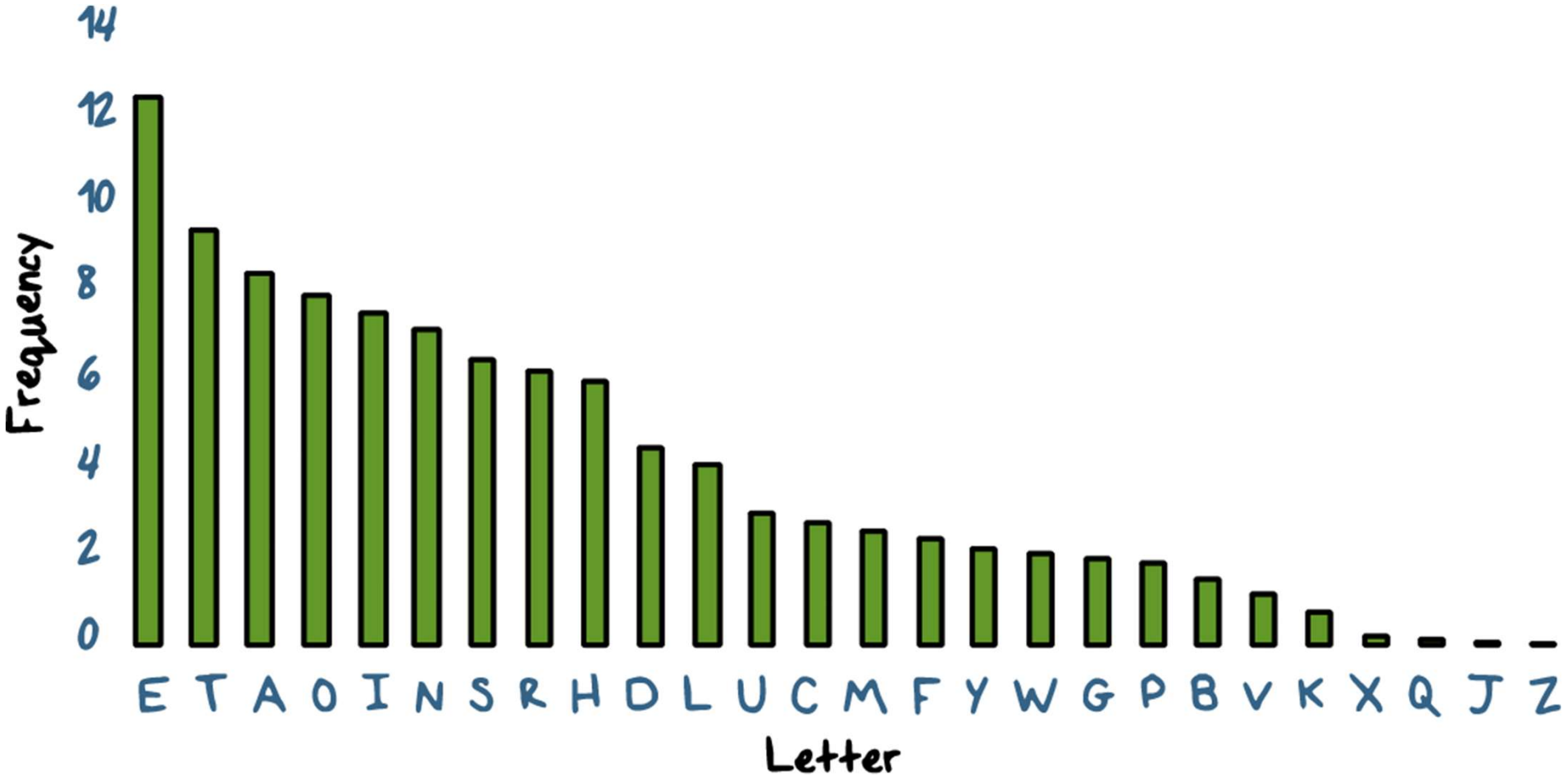
- **Brute-force attack**
  - E.g., try all possible keys
- **Cryptanalysis**
  - Analysis of the algorithm and data characteristics
- **Implementation attacks**
  - E.g., side channel analysis
- **Social-engineering attacks**

Simple Ciphers

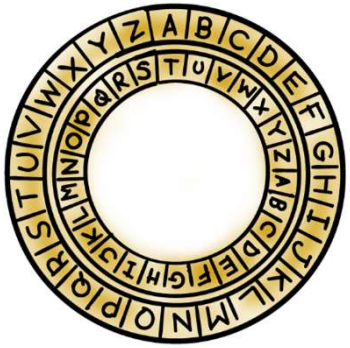


- **Caesar's cipher (or, shift cipher):**
  - E.g., A → D, B → E
  - That is, shift by an offset *n*:
    - (letter + *n*) mod 26
  - **only 26 possible ways** of secret coding
- **Monoalphabetic cipher (or, substitution cipher):**
  - **generalization**, arbitrary mapping of one letter to another
  - 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

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

What should be Kept Secret?

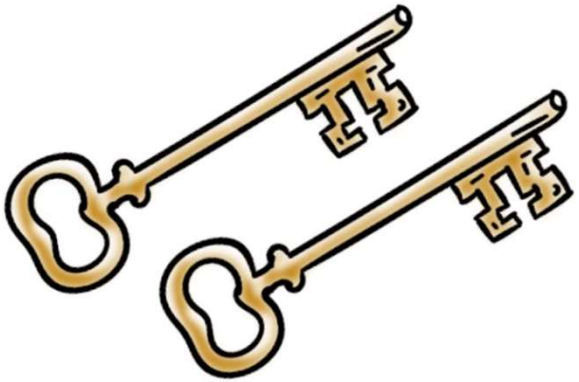
- **Kerckhoff's principle:**
  - A **cryptosystem** should be secure even if the attacker knows all details about the system, with exception of the secret key

- **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



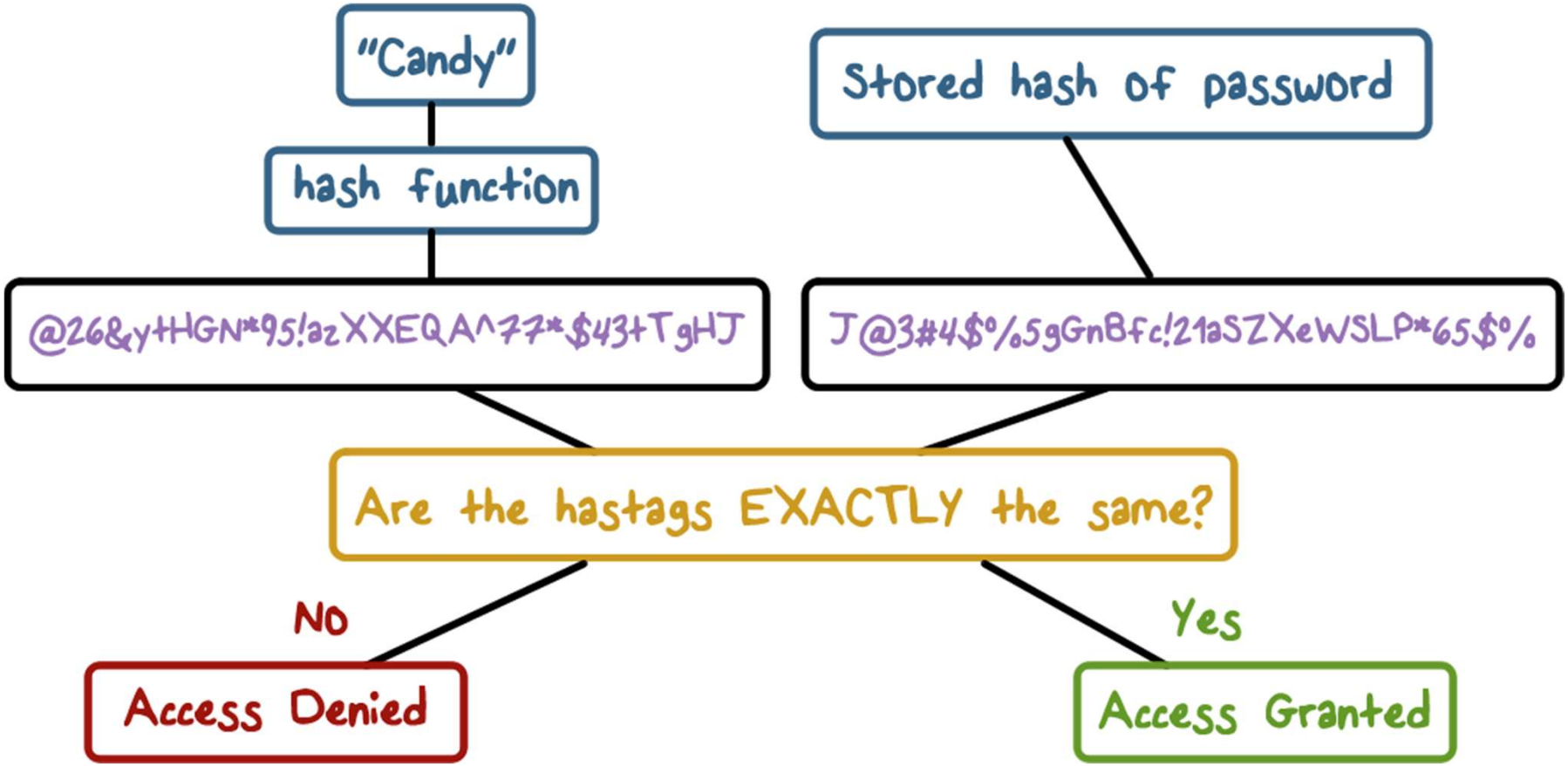
Public key cryptography:

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

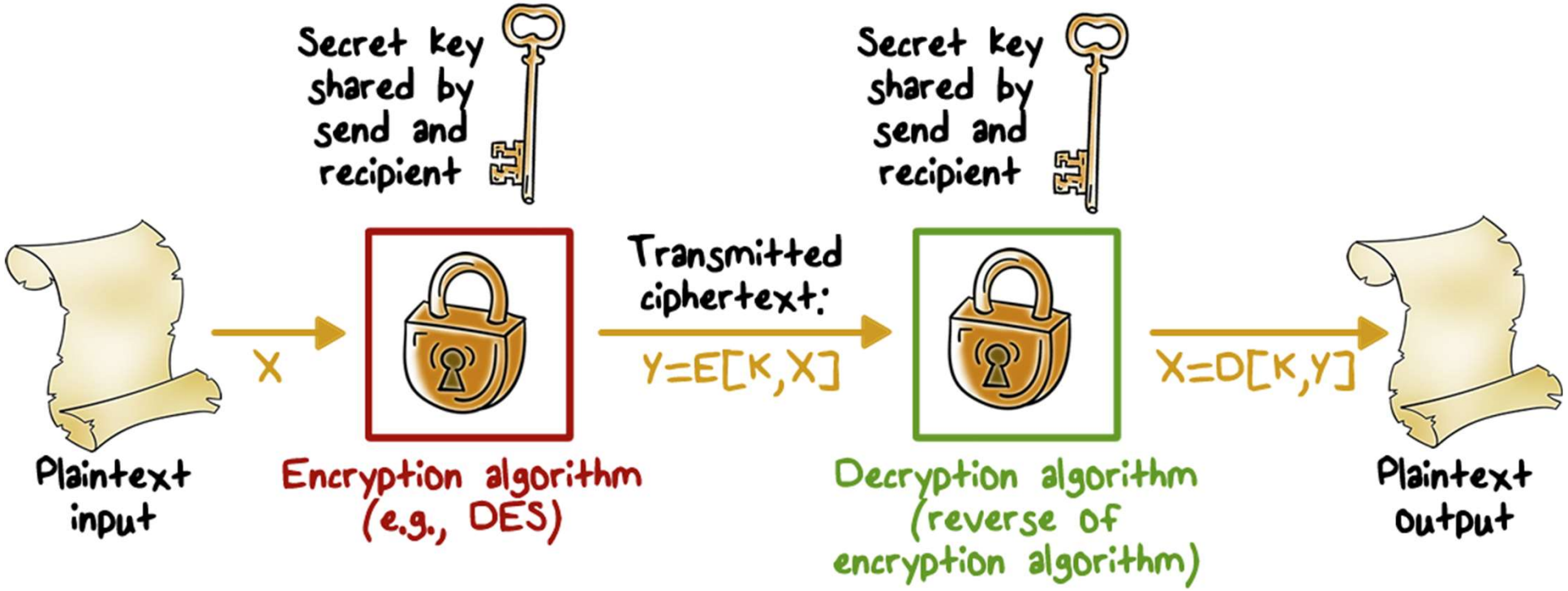
Hash Functions

- 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**

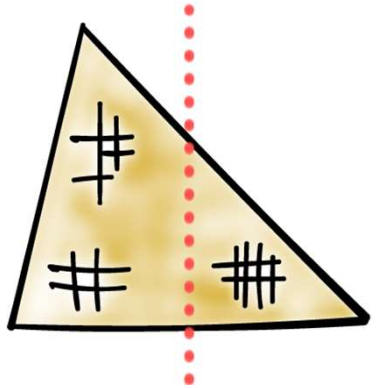
Hash Functions for Passwords



Symmetric Encryption

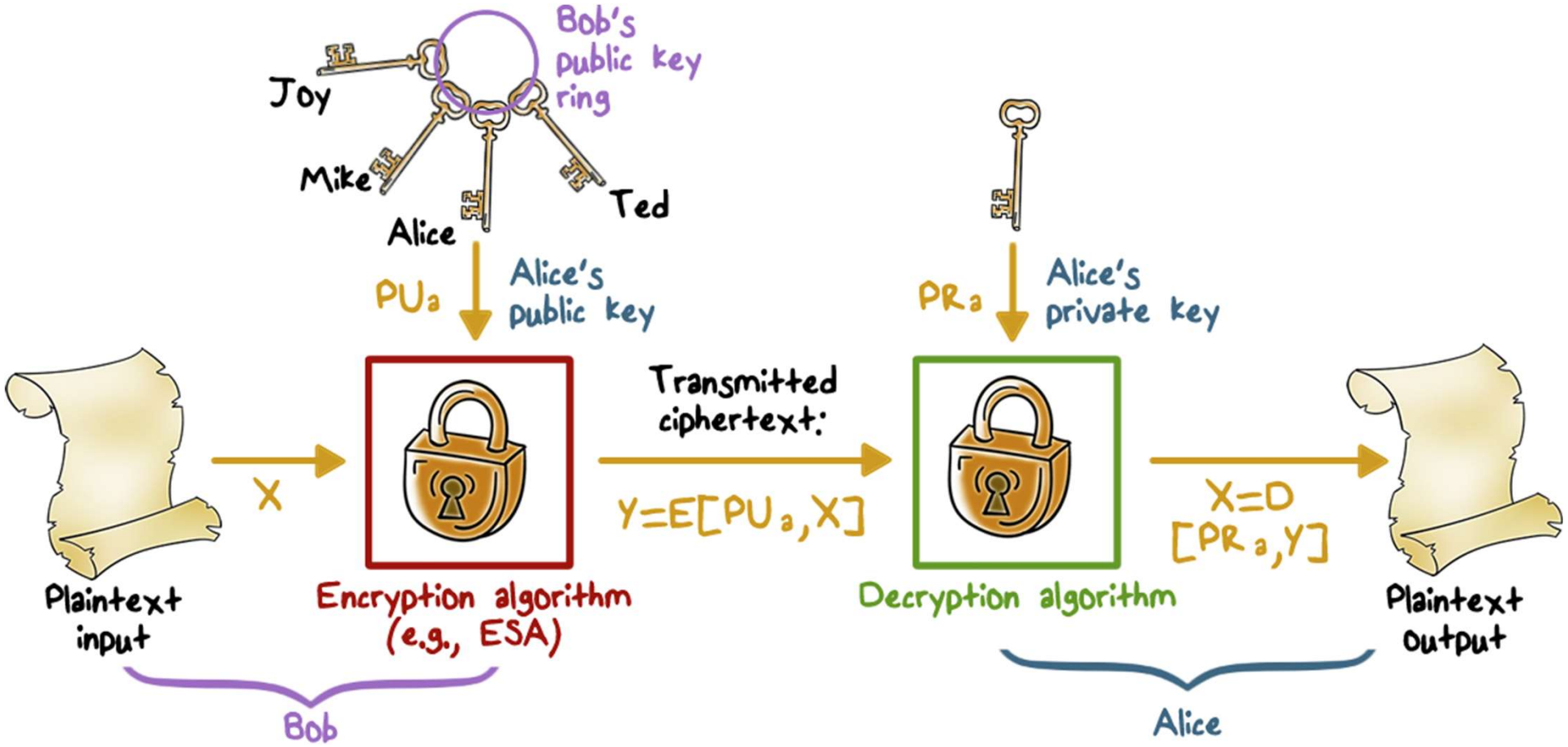


Asymmetric Encryption

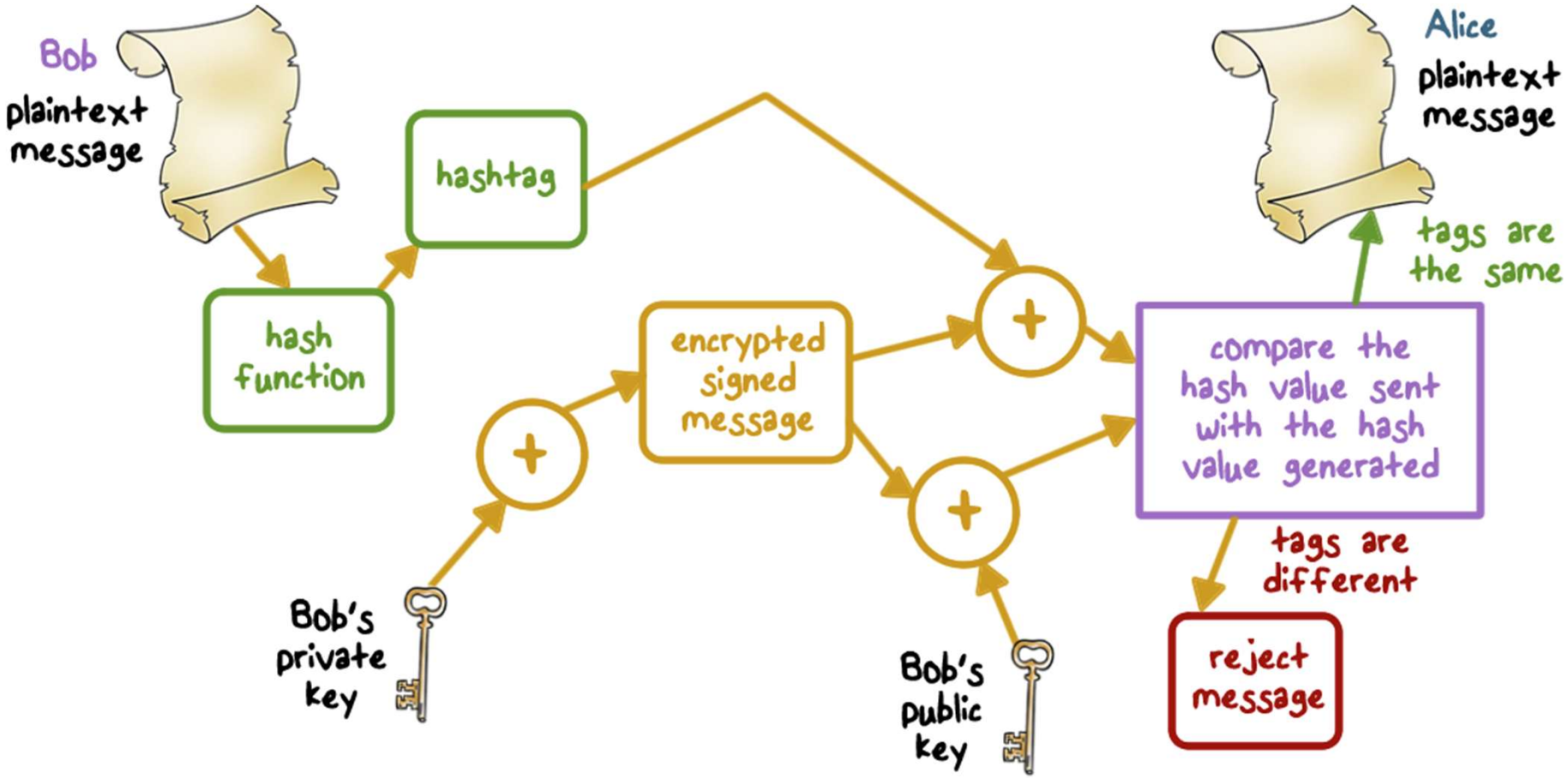


- **Plaintext**: Readable message or data that is fed into the algorithm
- **Encryption algorithm**: Performs transformations on the plaintext
- **Public and private key**: Pair of keys, one for encryption, one for decryption
- **Ciphertext**: Scrambled message produced as output
- **Decryption key**: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

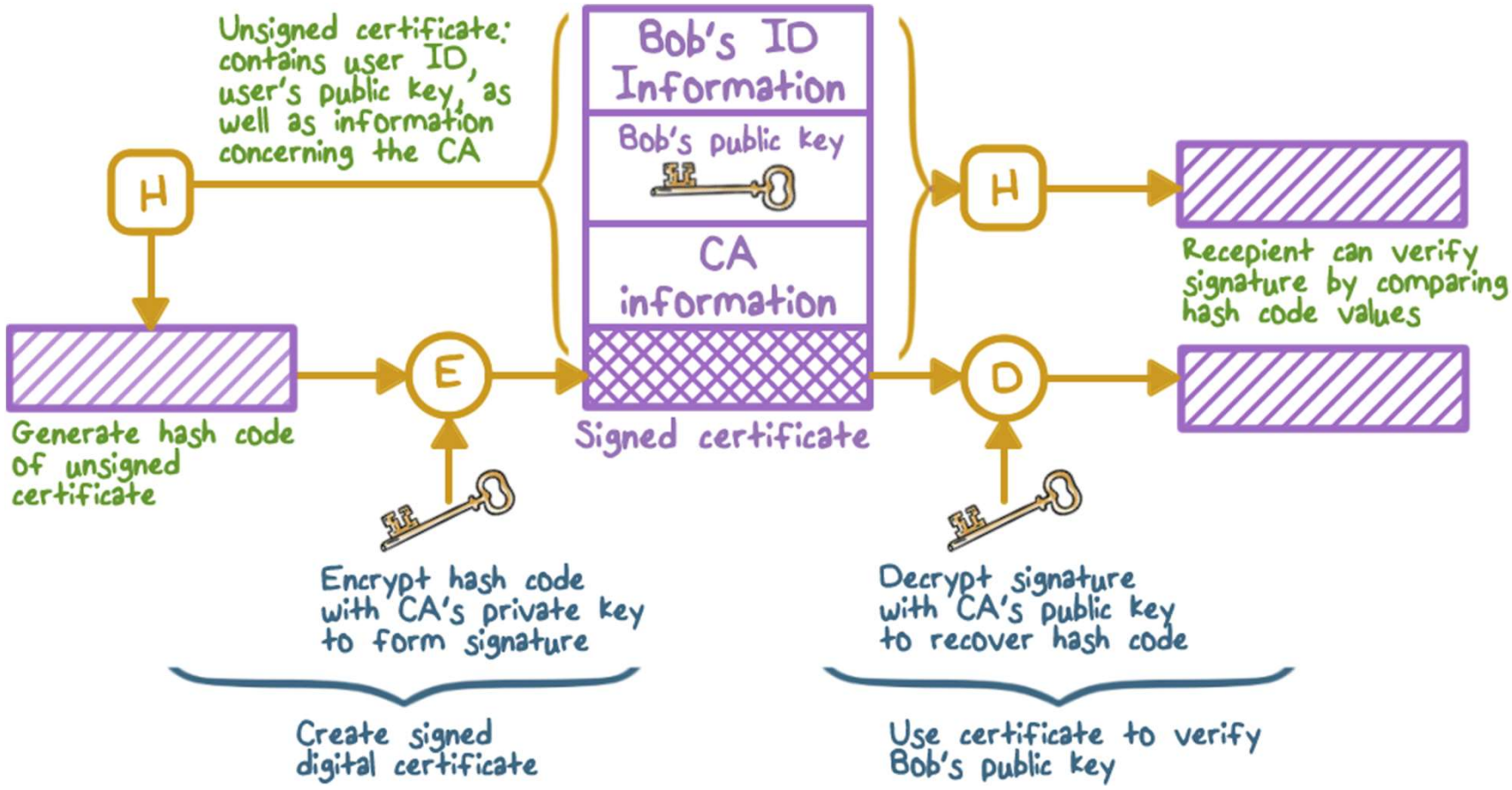
Asymmetric Encryption



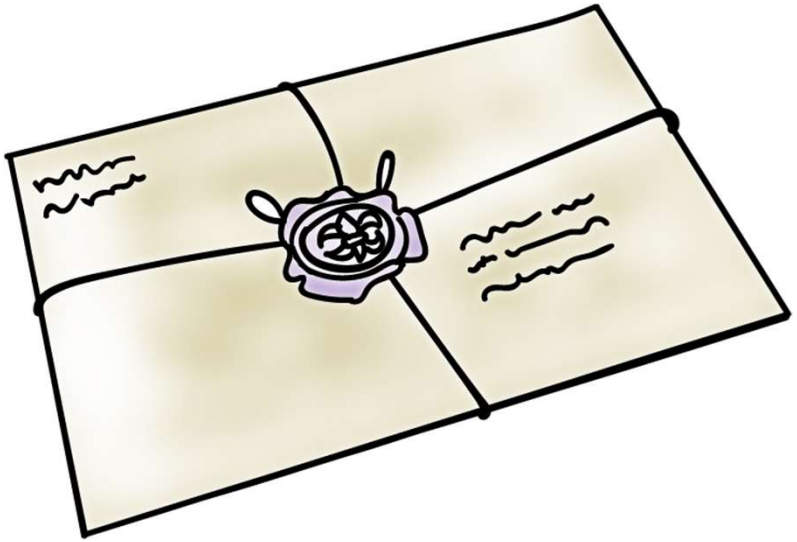
Digital Signatures



Digital Signatures

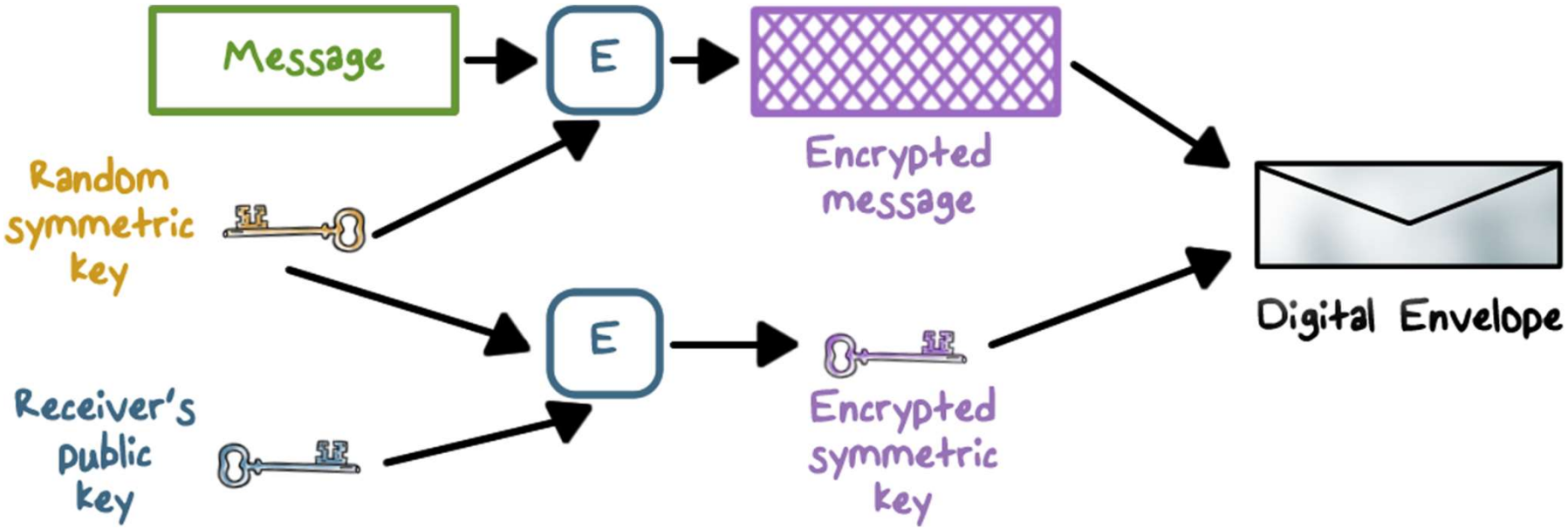


Digital Envelopes

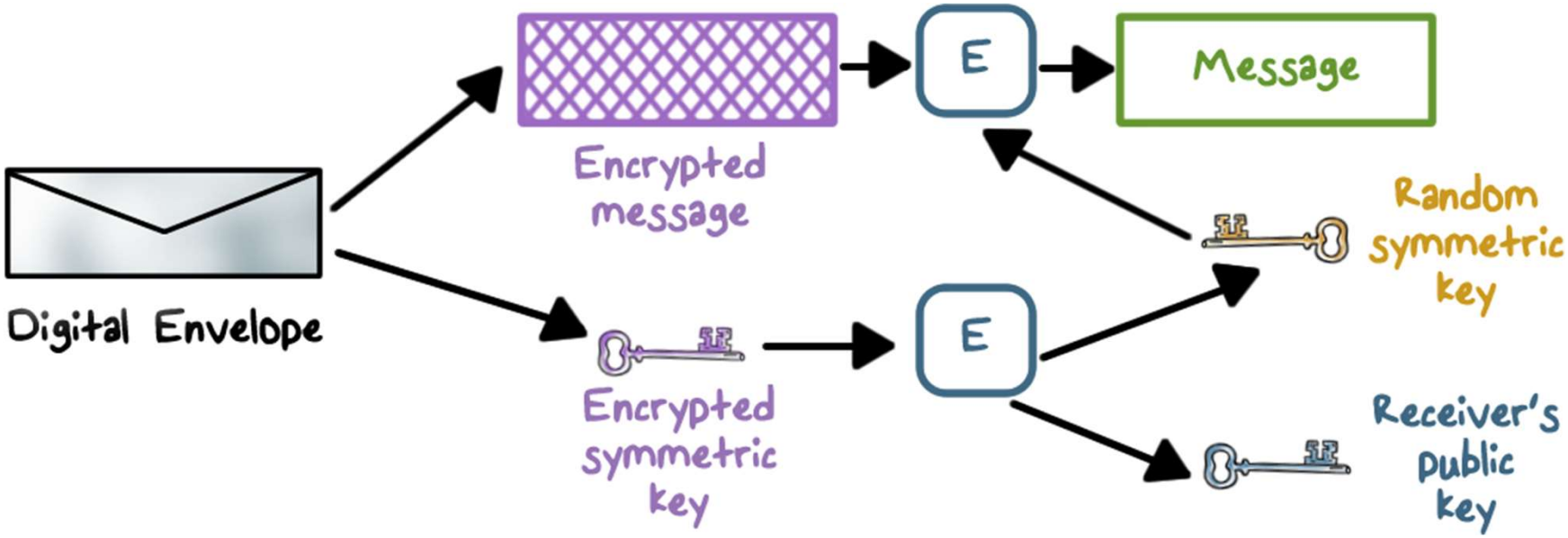


- Protects a message **without needing** to first arrange for sender and receiver to have the same secret key
- Equates to the same thing as a **sealed envelope containing an unsigned letter**

Digital Envelopes



Digital Envelopes



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