Cryptography

●●●

A Brief History and Introduction
MATH 314

What is cryptography?

$$\kappa\rho\upsilon\pi\tau\grave{o}\varsigma \quad \gamma\rho\grave{\alpha}\phi\omega$$

"hidden, secret"   "writing"
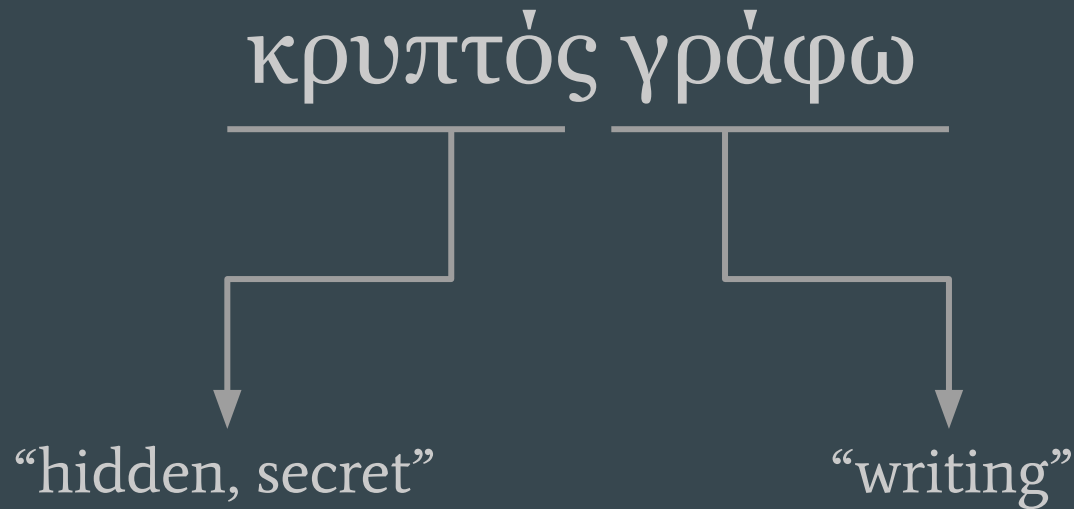
- **Cryptology**
  Study of communication securely over insecure channels
- **Cryptography**
  Writing (or designing systems to write) messages securely
- **Cryptanalysis**
  Study of methods to analyze and break hidden messages

Secure Communications

Encryption Key → Encrypt

Decryption Key → Decrypt

Alice → Encrypt → Decrypt → Bob

Plaintext (Alice → Encrypt)

Ciphertext (Encrypt → Decrypt)

Plaintext (Decrypt → Bob)

Eve
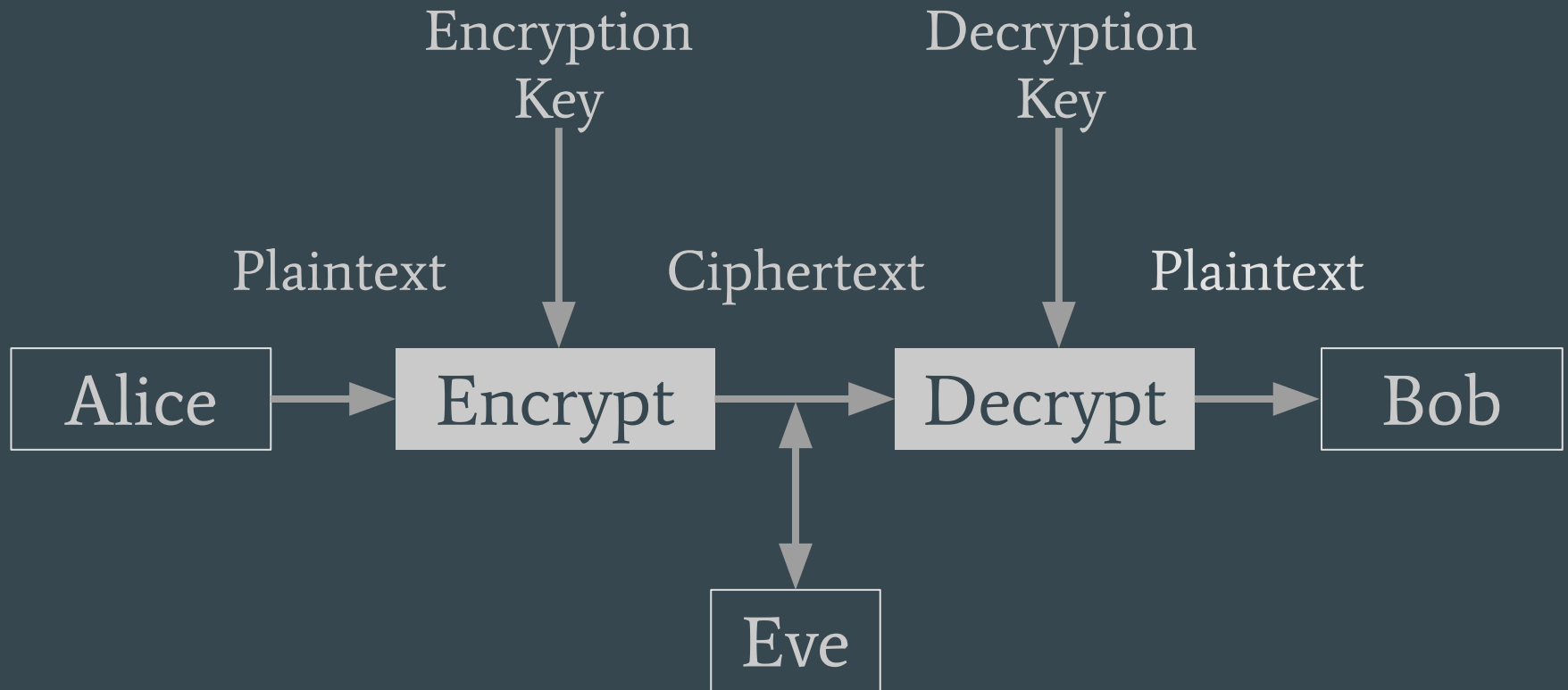
- **Symmetric Key:** Alice and Bob use a (preshared) secret key.
- **Public Key:** Bob makes an encryption key public that Alice uses to encrypt a message. Only Bob has the decryption key.

Possible Attacks

Eve (the eavesdropper) is trying to:

- Read Alice's message.
- Find Alice's key to read all of Alice's messages.
- Corrupt Alice's message, so Bob receives an altered message.
- Pretend to be Alice and communicate with Bob.

Why this matters

- **Confidentiality**
  Only Bob should be able to read Alice's message.
- **Data integrity**
  Alice's message shouldn't be altered in any way.
- **Authentication**
  Bob wants to make sure Alice actually sent the message.
- **Non-repudiation**
  Alice cannot claim she didn't send the message.

Going back in time...

5th century BC

Secret writing and **steganography** saved Greece from being completely conquered by the Persians.

- Invisible Ink
- Shaved head

Steganography vs. Cryptography

Steganography hides the existence of a message.

Cryptography hides the meaning of a message.

Back to 5th century BC

Lysander of Sparta used a scytale for encryption.

Back to 5th century BC

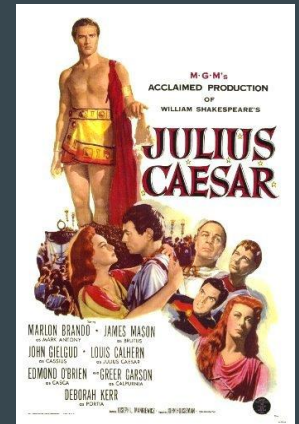The sender wraps the message around a rod of a fixed diameter.

Example: "Help me I am under attack."

H	E	L	P	M
E	I	A	M	U
N	D	E	R	A
T	T	A	C	K

HENTEIDTLAEAPMRCMUAK

- To decrypt, just wrap strip around a rod of the same diameter.

1st century BC

Julius Caesar used a cipher (now known as the "Caesar cipher")

Idea: Encrypt message by shifting the alphabet 3 letters.

Example: "Et tu, Brute?"

Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: DEFGHIJKLMNOPQRSTUVWXYZABC
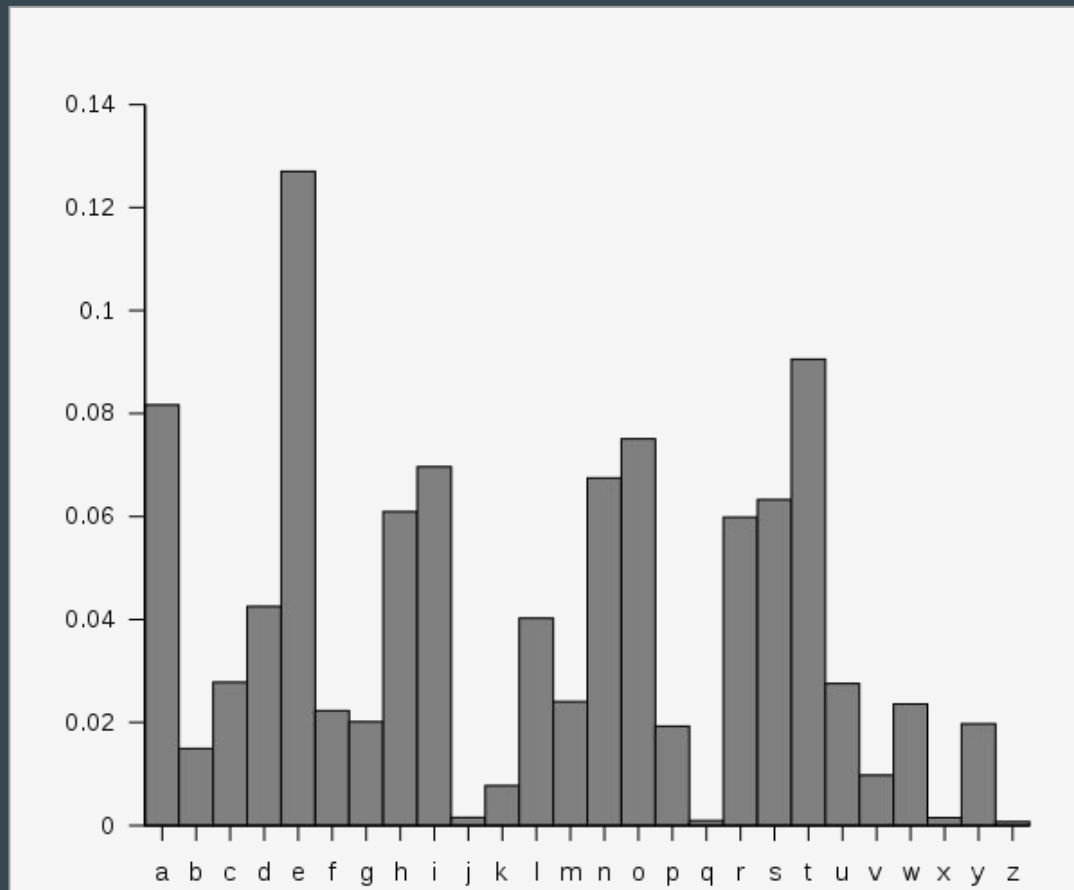

Plaintext: ETTUBRUTE
Ciphertext: HWWXEUXWH

9th-10th century

- *Adab-al-Kuttāb* or "The Secretaries' Manual"
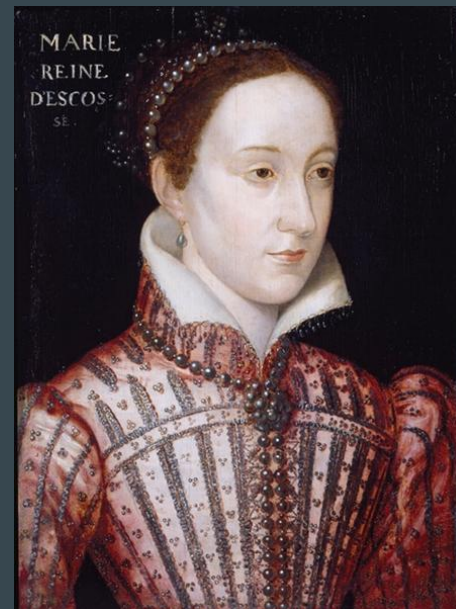- Arabs invented **cryptanalysis**, systematic study of ways of deciphering a code without a key.
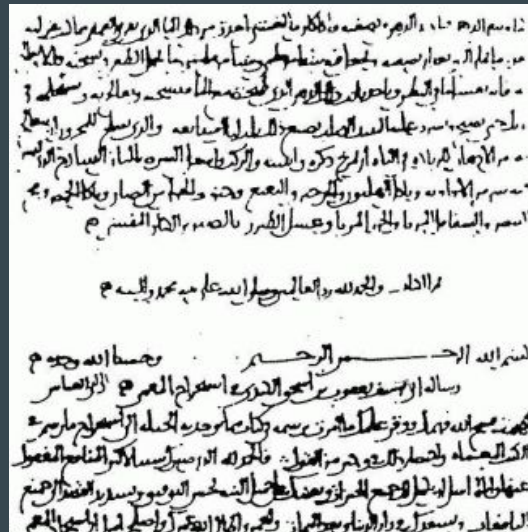
9th-10th century

Frequency analysis: Using frequently used letters to decipher the code.

15th century

- Use of **nulls** to confuse cryptanalysts.
- Used in Babington plot to assassinate Queen Elizabeth.
- Broken, let to the trial and execution of Mary, Queen of Scots

1586
Vigenère Cipher

Blaise de Vigenère reinvents Giovan Battista Bellaso's cipher.

One letter is no longer encoded the same way every time.

Described as unbreakable by many, including Lewis Carroll.

1586

Example: Encrypting "Attack at dawn" using LEMON

Plaintext: ATTACKATDAWN

Key: LEMONLEMONLE

Ciphertext: LXFOPVEFRNHR

1854

- Charles Babbage found a solution to the Vigenère cipher.
- Analytical Engine
- "Father of the Computer" along with Ada Lovelace

You can see half
his brain at the
Science Museum
in London!
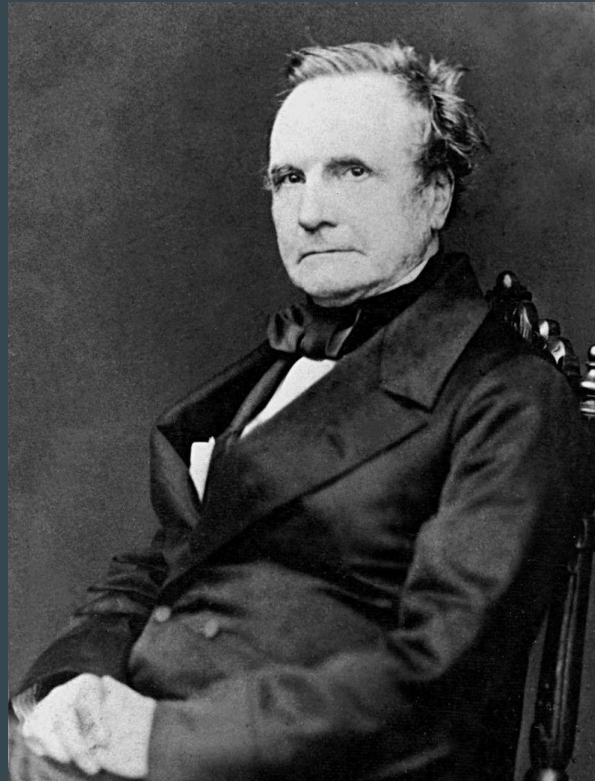
The other half is
at the Hunterian
Museum in the
Royal College of
Surgeons in
London.

1920s-1940's

- Enigma machines (Germany)
- Most notably used in WWII
- Polish Cipher Bureau started breaking Enigma messages.
- Alan Turing later improved the Polish methods.
- Bombe

You can try a working enigma machine at the cryptologic museum at Fort Meade.

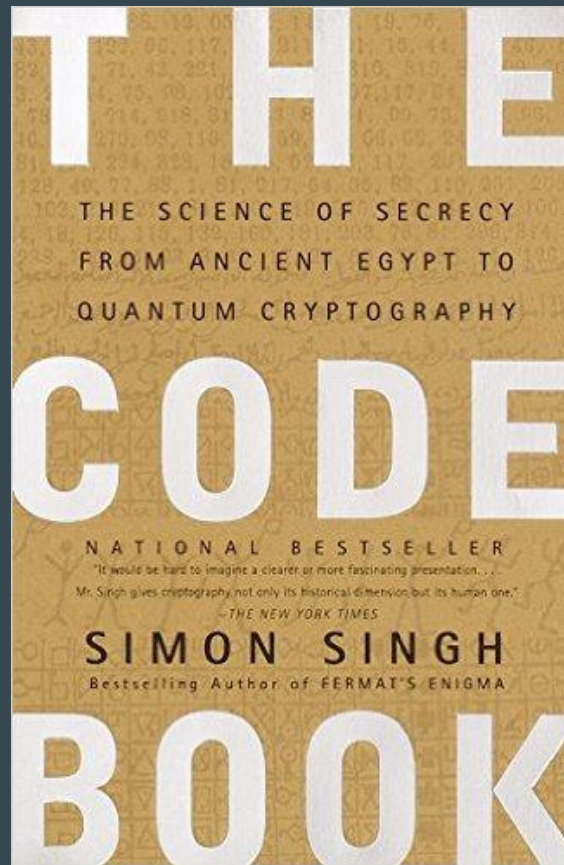# Recurring Theme (until the 1970s)

- Secret Code Invented.
- Typically called "unbreakable" by inventor.
- Used by spies, ambassadors, kings, generals for crucial tasks.
- Broken by enemy using cryptanalysis.

"Human ingenuity cannot concoct a cipher
which human ingenuity cannot resolve."

Edgar Allan Poe, 1841

If you want more history…

Read The Code Book (Simon Singh).

This Course

What you'll learn:

- Foundations and principles of the math behind crypto.
- Basic ingredients and components.
- Definitions, theorems and some proofs
- High-level applications and implementations

What you will not learn:

- The most efficient and practical versions of components.
- Designing secure systems
- "Hacking" – breaking into systems.
- Viruses, worms, side-channel attacks etc.
- Everything important about crypto

Resources

- Course Website: http://tigerweb.towson.edu/nmcnew/m314f23/
- CoCalc: http://www.cocalc.com/
- The textbook:

Christof Paar
Jan Pelzl

Understanding Cryptography

A Textbook for Students and Practitioners

Springer