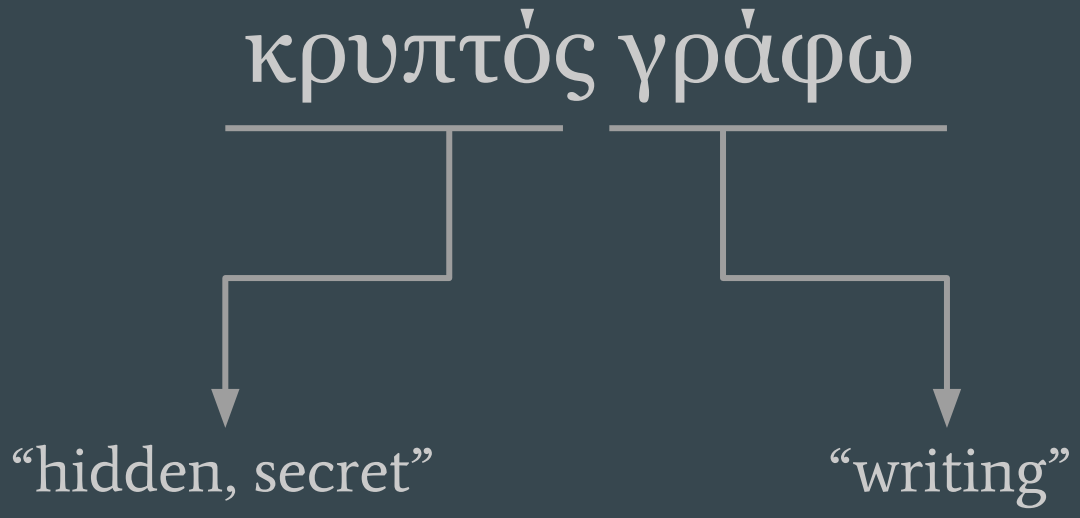
Cryptography

...

A Brief History and Introduction
MATH/COSC 314

Based on slides by Anne Ho
Carolina Coastal University

What is cryptography?

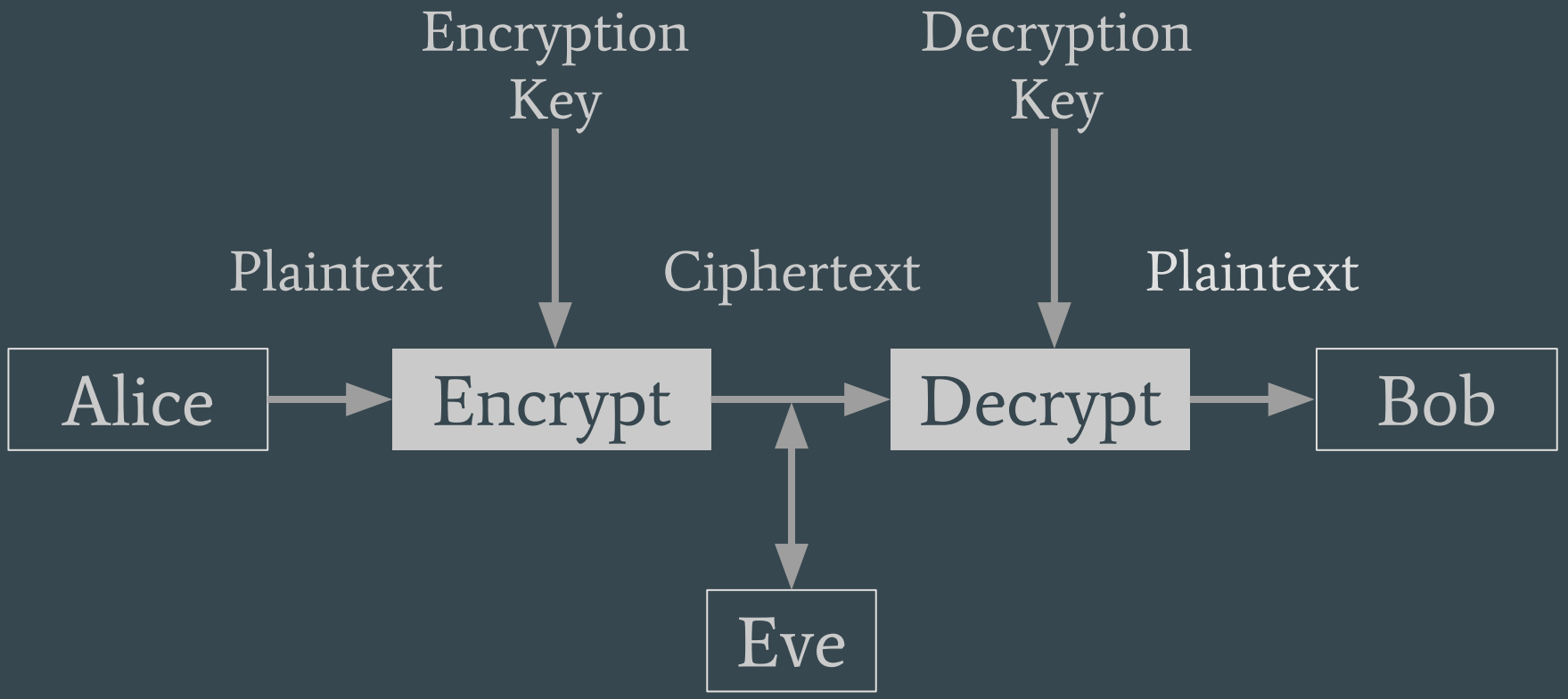


- **Cryptology**
  Study of communication securely over insecure channels
- **Cryptography**
  Writing (or designing systems to write) messages securely
- **Cryptanalysis**
  Study of methods to analyze and break hidden messages

Secure Communications

- Alice wants to send Bob a secure message.
- Examples:
  - Snapchat snap
  - Bank account information
  - Medical information
  - Password
  - Dossier for a secret mission (because Bob is a field agent for an intelligence agency and Alice is his boss)

Secure Communications



- **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.

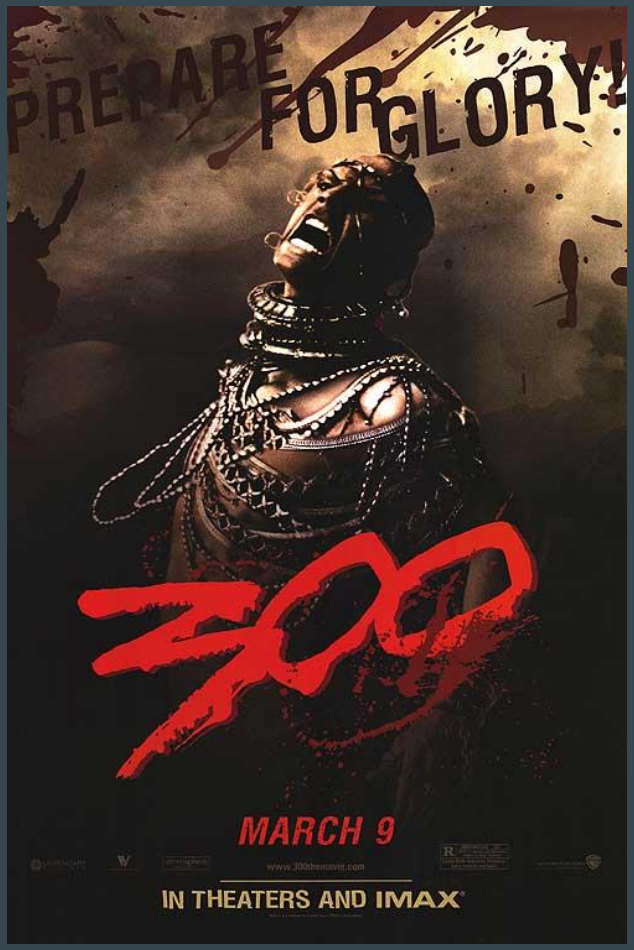
Why this matters

- **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

King Xerxes I of Persia

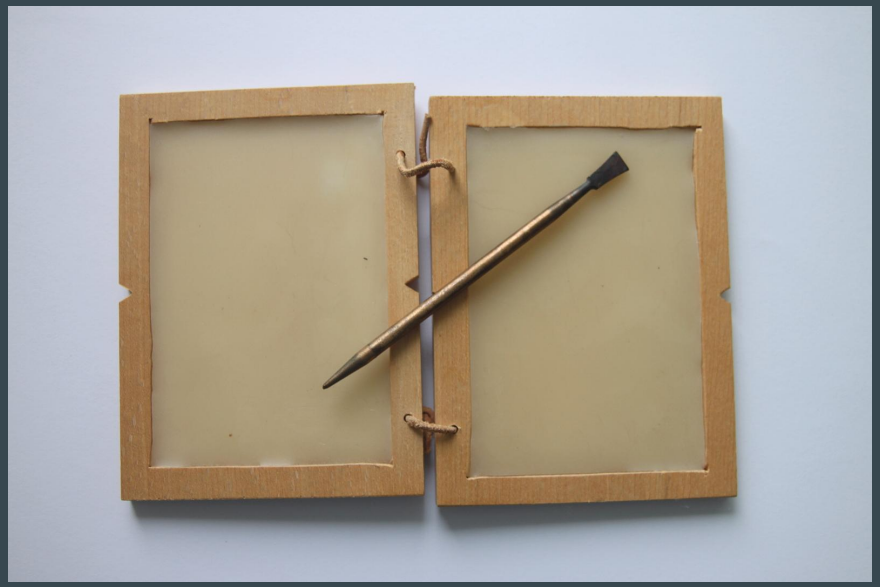


Definitely not historically accurate. Based on Frank Miller's graphic novel, not history.

5th century BC

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

- Wax tablet
- 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 certain diameter.

Example: “Help me I am under attack.”

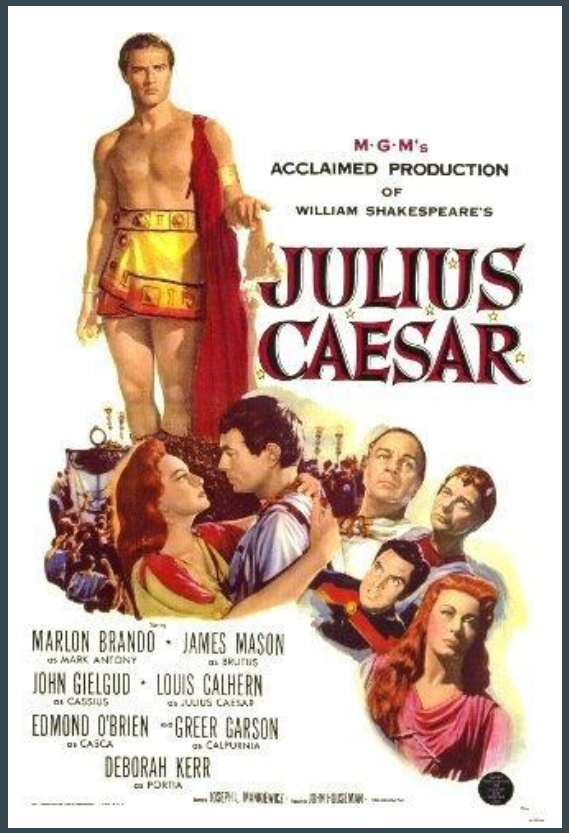
or

Back to 5th century BC

- The messenger brings the leather strip to the receiver.
- To decrypt, the receiver just has to wrap the leather strip around a rod of the same diameter.
- Possibly used for **authentication** instead of encryption since it's relatively easy to break.

1st century BC

Julius Caesar used a cipher (now known as the “Caesar cipher”)



Also dramatized. Based on the Shakespeare play.

1st century BC

Example: “Et tu, Brute?”

Plaintext: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
Ciphertext: `DEFGHIJKLMNOPQRSTUVWXYZABC`

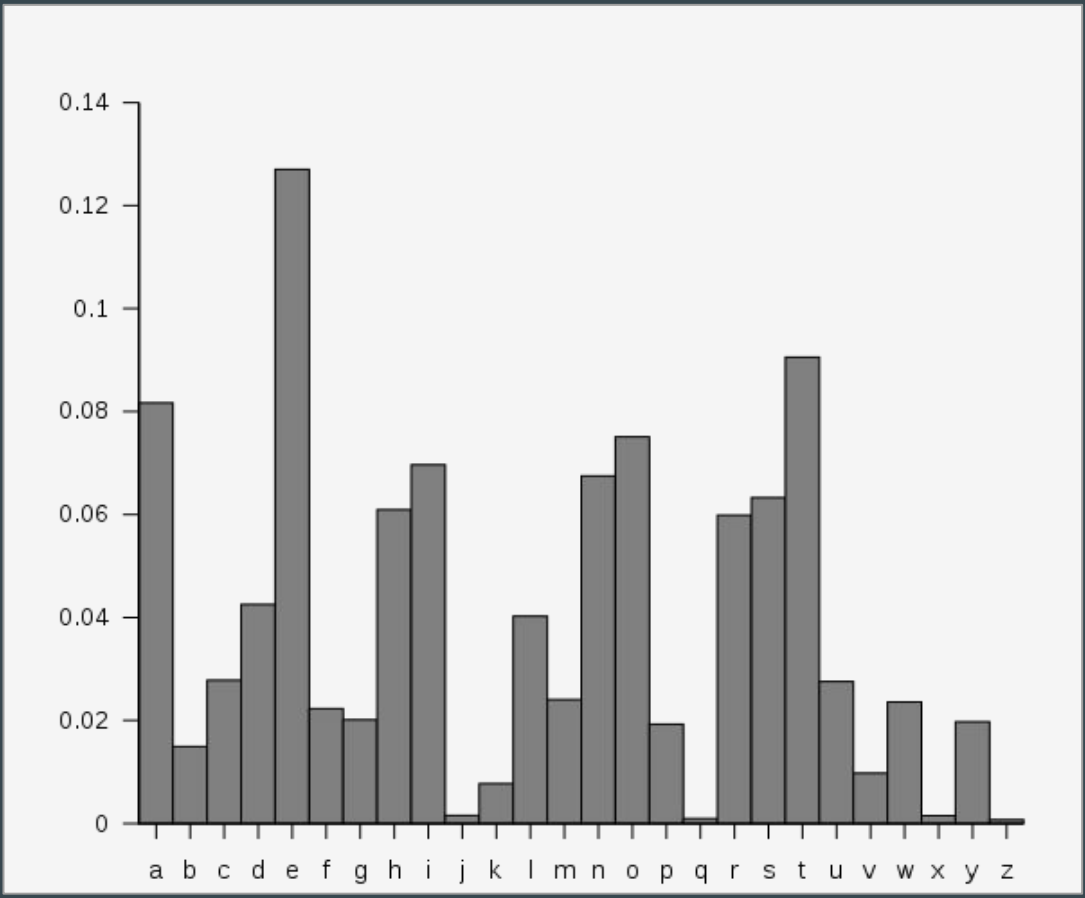
Plaintext: `ETTUBRUTE`
Ciphertext: `HWWXEUXWH`

9th-10th century

- Arab tax records
- *Adab-al-Kuttāb* or “The Secretaries’ Manual”
- Arabs invented **cryptanalysis**, systematic study of ways of deciphering a code without a key.
- Al-Kindi’s *A Manuscript on Deciphering Cryptographic Messages*

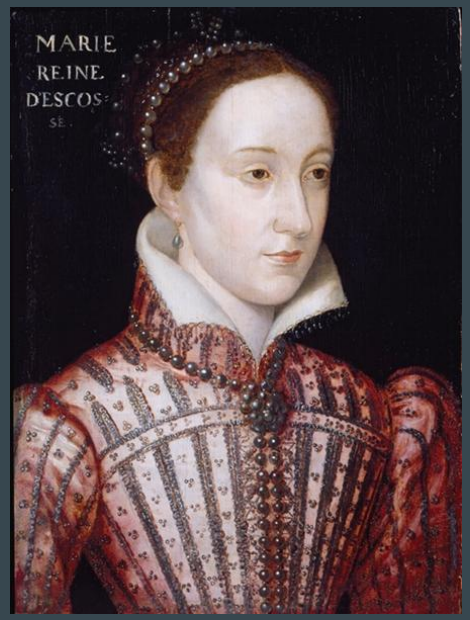
9th-10th century

Frequency Analysis: Comparing how frequently letters occur to decipher the code.



15th century

- Use of **nulls** to confuse cryptanalysts.
- Evidence in the Babington Plot (to assassinate Elizabeth)
- 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

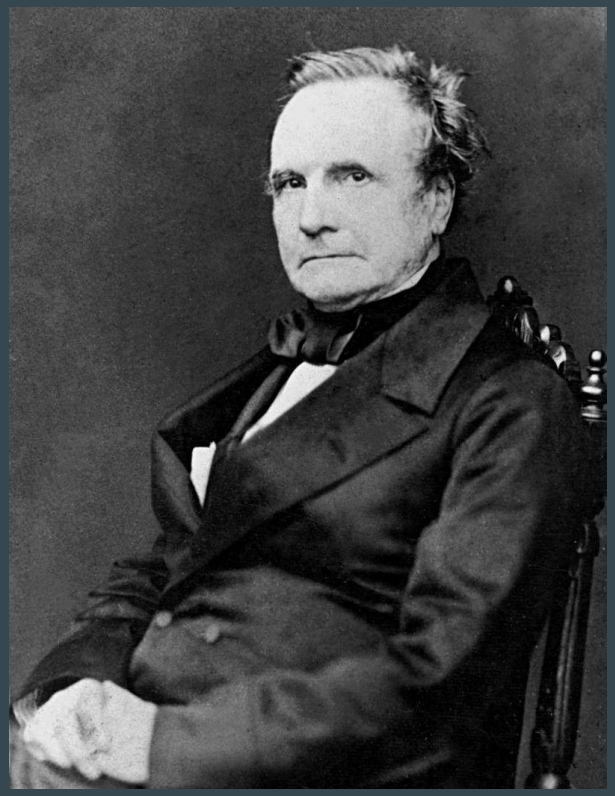
Ciphertext: LXFOPVEFRNHR

	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

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!



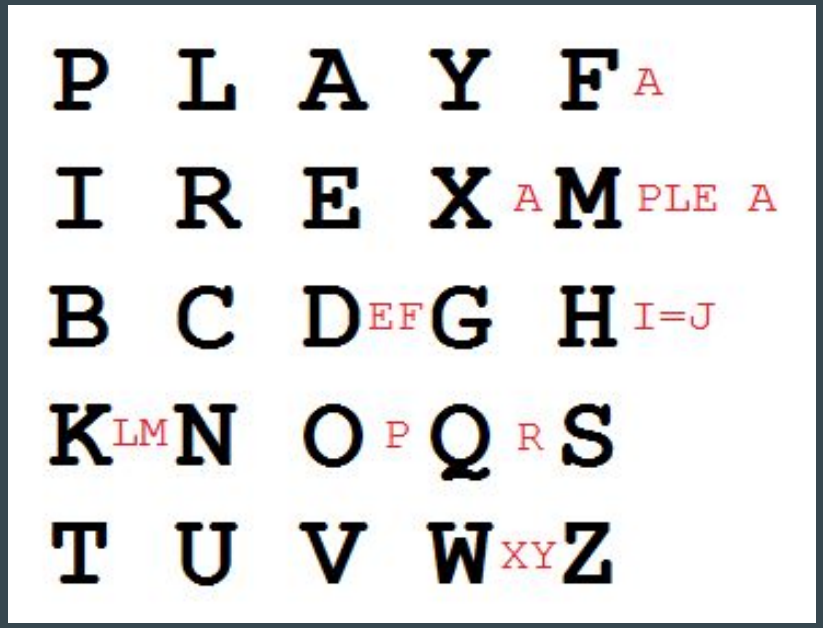
The other half is at the Hunterian Museum in the Royal College of Surgeons in London.

1854

- Playfair cipher invented by Sir Charles Wheatstone (but named after the Baron Playfair)
- Encrypts pairs of letters instead of single letters, so frequency analysis isn't as useful to break the cipher
- Used by the British in WWI.
- Uses a 5x5 table with a keyword or phrase.

1854

Example: “Playfair example”



1854

Encrypt “Hide the gold in the tree stump”

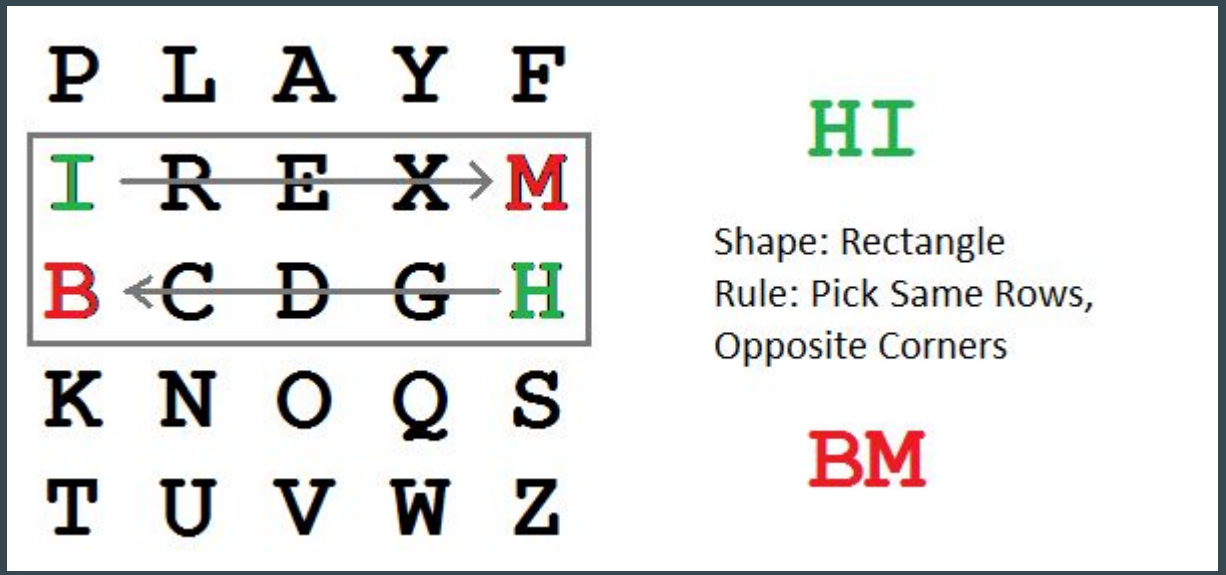
HI DE TH EG OL DI NT HE TR EX ES TU MP

X used to separate the repeated Es.

1854

Encrypt “Hide the gold in the tree stump”

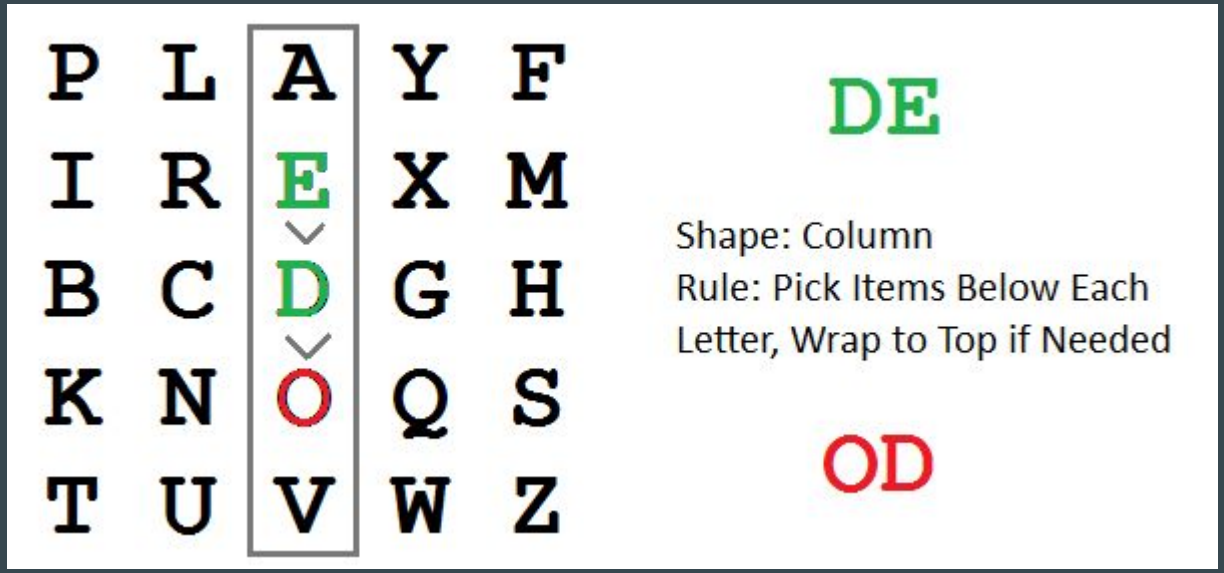
HI DE TH EG OL DI NT HE TR EX ES TU MP



1854

Encrypt “Hide the gold in the tree stump”

HI **DE** TH EG OL DI NT HE TR EX ES TU MP



1854

Encrypt “Hide the gold in the tree stump”

```
HI DE TH EG OL DI NT HE TR EX ES TU MP

BM OD ZB XD NA BE KU DM UI XM MO UV IF
```

Decrypting requires working backwards.

1885

Beale Ciphers

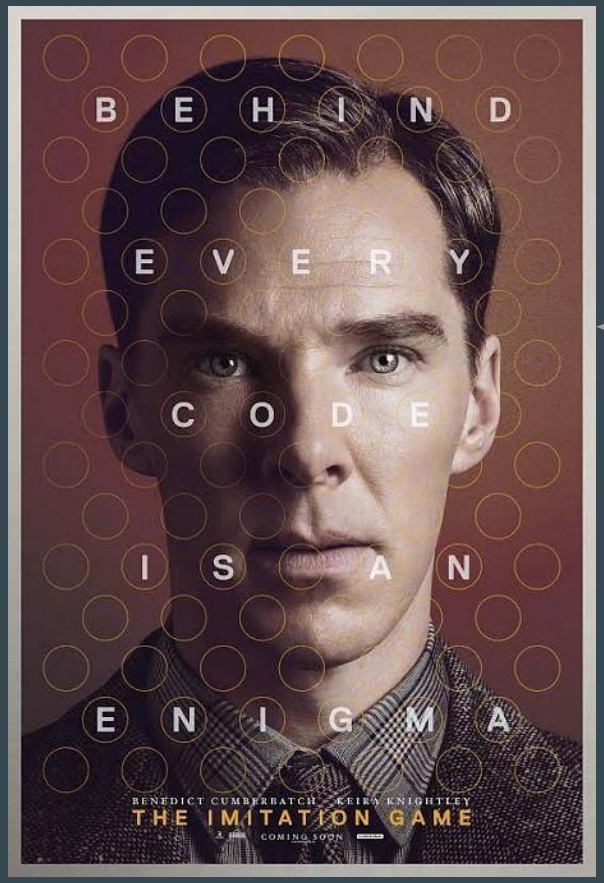
- Three ciphertexts which supposedly say the location of buried treasure (worth probably about $70 million now)
- Only the second ciphertext has been broken, and it was based on the Declaration of Independence.
- Truth or hoax?

1920s

- Enigma machines (Germany)
- Most notably used in WWII

1930s-1940s

- Polish Cipher Bureau started breaking Enigma messages.
- Alan Turing later improved the Polish methods.
- Bombe



More movie drama, but describes interesting history!

Recurring Theme (until the 1970s)

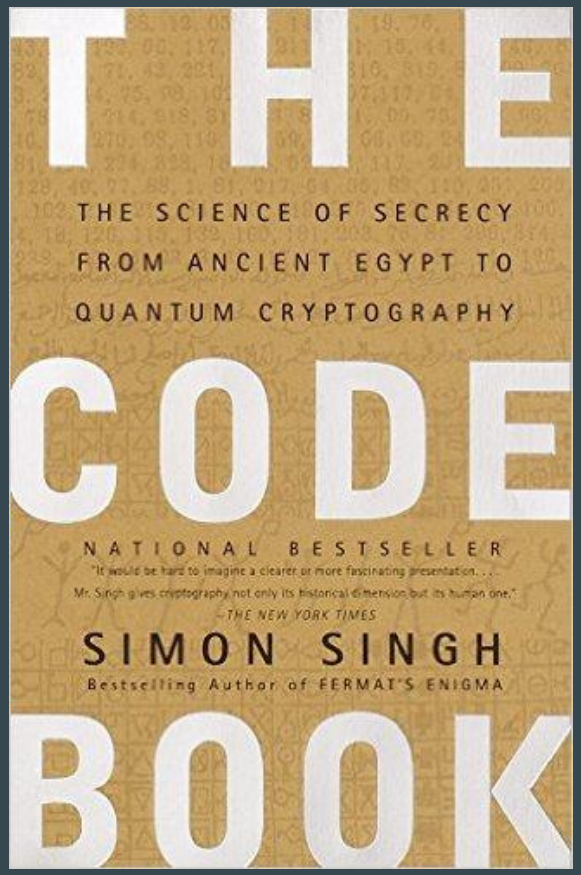
- Secret Code Invented.
- Typically called “unbreakable” by inventor.
- Used by spies, ambassadors, kings, generals for crucial tasks.
- Broken by enemy using cryptanalysis.

“Human ingenuity cannot concoct a cipher
which human ingenuity cannot resolve.”

Edgar Alan Poe, 1841

If you want more history…

Read The Code Book (Simon Singh) and Wikipedia.



2015-2016

- December 2015: San Bernardino attack
- February 2016: The FBI ordered Apple to unlock an iPhone with a passcode. The phone belonged to one of the shooters of the attack. Apple refused to comply (backdoor issue).
- March 2016: The FBI said they had help from a third-party.
- April 2016: Burr-Feinstein Bill proposed.

This Course

What you'll learn:

- Foundations and principles of the science
- Basic ingredients and components.
- Definitions and proofs of security
- High-level applications

What you will not learn:

- The most efficient and practical versions of components.
- Designing secure systems*
- "Hacking" – breaking into systems.
- Viruses, worms, Windows/Unix bugs, buffer overflow etc..
- Everything important about crypto

The next few months…

- You are a secret-agent-in-training for the intelligence agency known as MATH/COSC 314.
- You will be given a **series of missions (assignments)** to be done in class and outside of class.
- There will be **three priority missions (exams)** for you to show your skills and growing body of secret agent knowledge.
- You primary goal is to **solve problems**, so utilize the resources you have (i.e. me, your classmates, and the textbook)!

Resources

- Course Website: http://tigerweb.towson.edu/nmcnew/m314f16/
- SageMath: http://cloud.sagemath.org/
- The textbook: