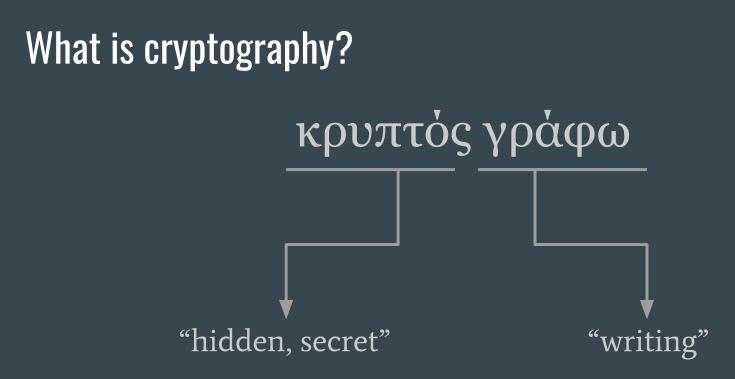
Cryptography

$\bullet \bullet \bullet$

A Brief History and Introduction MATH/COSC 314

> Based on slides by Anne Ho Carolina Coastal University



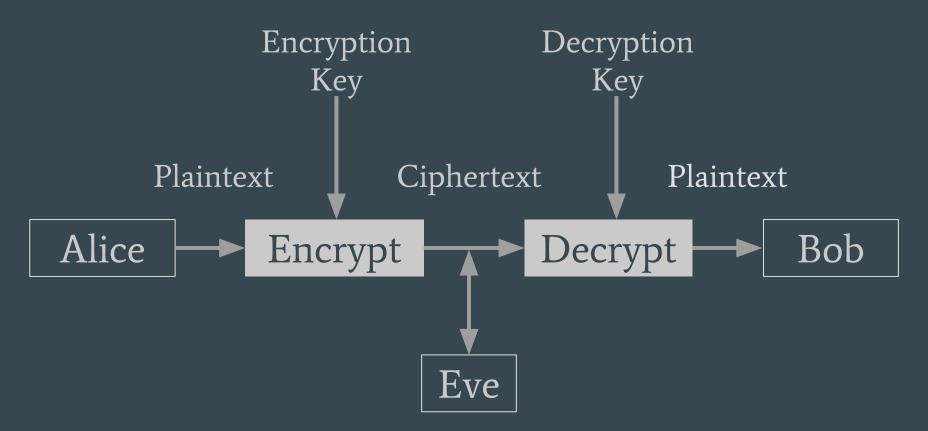
• Cryptology

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



- **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

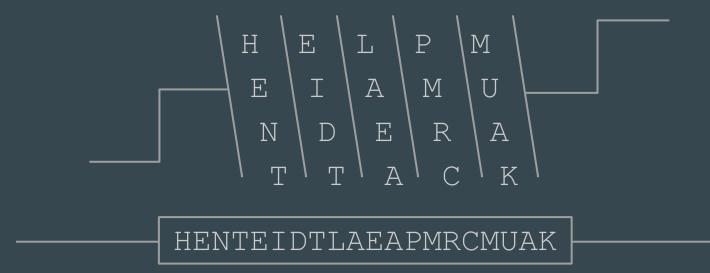
Lysander of Sparta used a scytale for encryption.



Back to 5th century BC

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

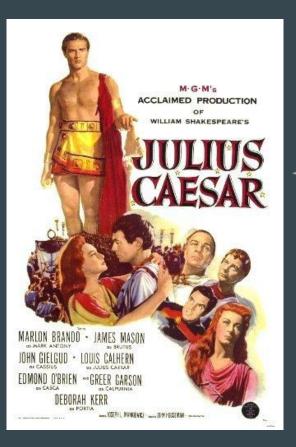
Example: "Help me I am under attack."



• 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")



Dramatized based on the Shakespeare play.

1st century BC

Caesar Cipher: Encrypt message by shifting the alphabet 3 letters.

Example: "Et tu, Brute?"

Plaintext:ABCDEFGHIJKLMNOPQRSTUVWXYZCiphertext:DEFGHIJKLMNOPQRSTUVWXYZABC

Plaintext: ETTUBRUTE Ciphertext: HWWXEUXWH

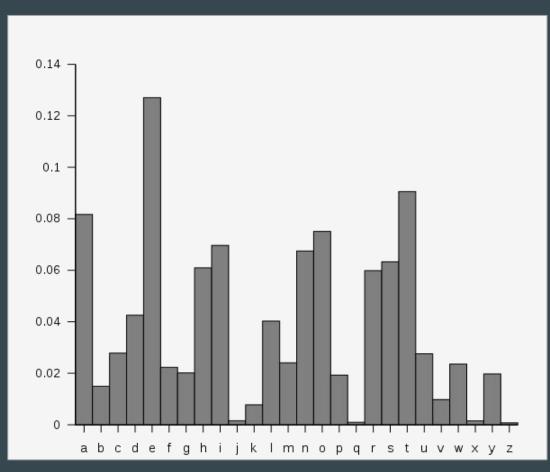
9th-10th century

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

دا. معالده ما در الدجر وجف ماطلومالغ تتواحدة مرد الدالدي مراجع موالد عرف. مر جاعارات معاد معد مقد فعرف خاص مد تعام الموت المهمة ما المقد ومعت طلامة - ما - مسلماد الطروباحول والإجرائة فتوضع المامسي وعالم وسعالي 1 ، لم مسجد عبد المسالي الم الم مع والعلد المساحد والدوسل المحرود المعلى - مالجعا لعملاء والعاد أدلي وكرد والمد، والرك على السره لله المسالة المراهم مدسم المراديد ويلا أعلمون للرحد والعمع وحن وللم لر الصار وبالالد ومج " فرااداد والحداله ردائعال محصلوا ليستعلم مدعد والمسه ع Paralle or 9 لسمالد الرح وسالدا وجسع يعور المحد الدوك استعراح المعرج الاوهاس عهد معالد فهما ووفر علما ماتم ويسمه وكمات كمودر الحدل المسعلة مارس لحمل العدد مزاهنا فالوله الارسيل سالالرالمنام الفعول المال المح المراز ومعذ كم النه المدومة ومسايد الفندا اح

9th-10th century

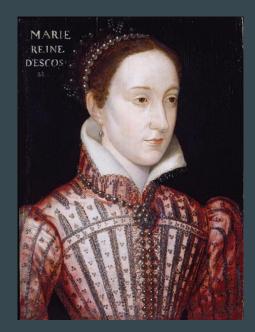
Frequency Analysis: Comparing how frequently letters occur to decipher the code.



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.

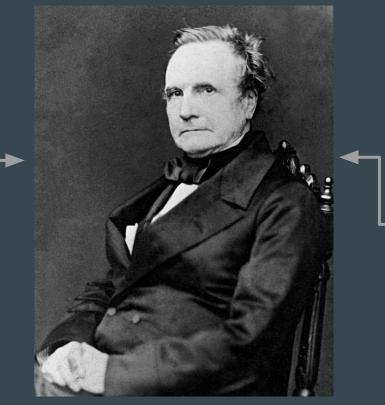
1586 Example: Encrypting "Attack at dawn" using LEMON

		A	BC	D	E	F	GΗ	1	J	K L	M	Ν	0	ΡQ	R	S	T	U١	W	X	Y Z	Ζ
														1000								
	1000	D																				
	E	E																				-
	F																					
A'I''I'ACKA'I'DAWN																						
T.E.MONT.E.MONT.E.	ĸ	-																				
																						_
LVLOLATKNUK	0																					
																						_
	100000000000000000000000000000000000000																					100
	ATTACKATDAWN LEMONLEMONLE LXFOPVEFRNHR	A TTACKATDAWN LEMONLEMONLE LXFOPVEFRNHR Q R S T U V W X Y	A A B B C C D D E E F F F F F F F F F F F F F F F F	A A B C B B C D C C D E D D E F E E F G F F G H I I J I I J K LEMONLEMONLE LXFOPVEFRNHR N N 0 N N 0 N N 0 P P Q R S T S S T U U U V W V W X V W X V W X V W X V V W X V V W X V V W X V V V V V V V V V V V V V V V V V V V	A A B C D B B C D E F C C D E F G D D E F G H F F G H I J K LEMONLEMONLE K K L M N LXFOPVEFRNHR N N O P Q Q Q R S T U S T U V V V Q Q R S T U V V V V V V V V V V V V V V V V V Z A P Z A	A A B C D E B B C D E F G C C D E F G H E E F G H I J F F G H I J K LEMONLEMONLE K K L M N O LXFOPVEFRNHR N N O P Q R Q R S T U V V V Q R S T U V V V V V V V V V V V V V V V V V V V V V V V V V V V L M N O P Q R S T V V V V V V	A A B C D E F G B B C D E F G H D D E F G H I J K C C D E F G H I J K L D D E F G H I J K L M N I J K L M N O C I I J K L M N O I I J K L M N O I I I J K L M N O I I I J K L M N O I I I I I I I I N N O I I I I I I N N O I N N I I	A A B C D E F G H I B B C D E F G H I J C C D E F G H I J K L D D E F G H I J K L A M N J K L M N J K L C C D E F G H I J K L M D D K K L M N O P L I J K L M N O P Q R S T U V	A A B C D E F G H I J B B C D E F G H I J K L C C D E F G H I J K L M D D E F G H I J K L M N O P C C D E F G H I J K L M N O P C G H I J K L M N O P Q R S T U N O P Q R S T U V <td< td=""><td>A A B C D E F G H I J B B C D E F G H I J K L D D E F G H I J K L M N D D E F G H I J K L M N O G G H I J K L M N O P H H J K L M N O P Q R S T U W N O P Q R S T U W W V W N O P Q R S T U W W W W W W W W W W W W W W W W W W W <td< td=""><td>A A B C D E F G H I J K L B B C D E F G H I J K L M N O C C D E F G H I J K L M N O P D D E F G H I J K L M N O P Q R F F G H I J K L M N O P Q R S T U V N O P Q R S T U V N</td><td>A A B C D E F G H I J K L M N C C D E F G H I J K L M N O D D E F G H I J K L M N O P C C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U V</td><td>A A B C D E F G H I J K L M N O C C D E F G H I J K L M N O P C C D E F G H I J K L M N O P Q C C D E F G H I J K L M N O P Q R S T U N N P Q R S T U V<!--</td--><td>A A B C D E F G H I J K L M N O B B C D E F G H I J K L M N O P Q C C D E F G H I J K L M N O P Q R D D E F G H I J K L M N O P Q R S T U V<!--</td--><td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W N V N N P Q R S T U V W X Y Z A B C D R S T U V W X Y Z A B C D R S T U V W<!--</td--><td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R S T D D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W Y Z D V W Y Z D V W X Y Z A B C D P Q R S T U V W X Y Z A B C D D D Q R S<!--</td--><td>A A B C D E F G H I J K L M N O P Q R S B B C D E F G H I J K L M N O P Q R S T U C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V E F G H I J K L M N O P Q R S T U V W F F G H I J K L M N O P Q R S T U V W G G H I J K L M N O P Q R S T U V W X Y G G H I J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B C D C D P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L W W X Y Z A B C D E F G H I J K L <td>A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C</td></td></td></td></td></td></td<><td>A A B C D E F G H I J K L M N O P Q R S T U V W B B C D E F G H I J K L M N O P Q R S T U V W X D D E F G H I K L M N O P Q R S T U V W Y Z A D D E F G H I J K L M N P Q R S T U W X Z A B C D D L M N D Q R S T U W X Z A B C D D L M N</td></td></td<> <td>A A B C D E F G H I J K L M N O P Q R S T U V W 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 D D E F G H I J K L M N O P Q R S T U 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 X Y Z A B C D D L L M N O P Q R S T U W X Z<td>A A B C D E F G H I J K L M N O P Q R S T U 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 W X Y Z A D D E F G H I K L M N O P Q R S T U W X Y Z A B C D E F G H I K L M N O P Q R S T U W X Z A B C D E G G H I J K L M N O P R S U W<td>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 B 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 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 C D E F G H I J K</td></td></td>	A A B C D E F G H I J B B C D E F G H I J K L D D E F G H I J K L M N D D E F G H I J K L M N O G G H I J K L M N O P H H J K L M N O P Q R S T U W N O P Q R S T U W W V W N O P Q R S T U W W W W W W W W W W W W W W W W W W W <td< td=""><td>A A B C D E F G H I J K L B B C D E F G H I J K L M N O C C D E F G H I J K L M N O P D D E F G H I J K L M N O P Q R F F G H I J K L M N O P Q R S T U V N O P Q R S T U V N</td><td>A A B C D E F G H I J K L M N C C D E F G H I J K L M N O D D E F G H I J K L M N O P C C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U V</td><td>A A B C D E F G H I J K L M N O C C D E F G H I J K L M N O P C C D E F G H I J K L M N O P Q C C D E F G H I J K L M N O P Q R S T U N N P Q R S T U V<!--</td--><td>A A B C D E F G H I J K L M N O B B C D E F G H I J K L M N O P Q C C D E F G H I J K L M N O P Q R D D E F G H I J K L M N O P Q R S T U V<!--</td--><td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W N V N N P Q R S T U V W X Y Z A B C D R S T U V W X Y Z A B C D R S T U V W<!--</td--><td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R S T D D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W Y Z D V W Y Z D V W X Y Z A B C D P Q R S T U V W X Y Z A B C D D D Q R S<!--</td--><td>A A B C D E F G H I J K L M N O P Q R S B B C D E F G H I J K L M N O P Q R S T U C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V E F G H I J K L M N O P Q R S T U V W F F G H I J K L M N O P Q R S T U V W G G H I J K L M N O P Q R S T U V W X Y G G H I J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B C D C D P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L W W X Y Z A B C D E F G H I J K L <td>A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C</td></td></td></td></td></td></td<> <td>A A B C D E F G H I J K L M N O P Q R S T U V W B B C D E F G H I J K L M N O P Q R S T U V W X D D E F G H I K L M N O P Q R S T U V W Y Z A D D E F G H I J K L M N P Q R S T U W X Z A B C D D L M N D Q R S T U W X Z A B C D D L M N</td>	A A B C D E F G H I J K L B B C D E F G H I J K L M N O C C D E F G H I J K L M N O P D D E F G H I J K L M N O P Q R F F G H I J K L M N O P Q R S T U V N O P Q R S T U V N	A A B C D E F G H I J K L M N C C D E F G H I J K L M N O D D E F G H I J K L M N O P C C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U V	A A B C D E F G H I J K L M N O C C D E F G H I J K L M N O P C C D E F G H I J K L M N O P Q C C D E F G H I J K L M N O P Q R S T U N N P Q R S T U V </td <td>A A B C D E F G H I J K L M N O B B C D E F G H I J K L M N O P Q C C D E F G H I J K L M N O P Q R D D E F G H I J K L M N O P Q R S T U V<!--</td--><td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W N V N N P Q R S T U V W X Y Z A B C D R S T U V W X Y Z A B C D R S T U V W<!--</td--><td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R S T D D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W Y Z D V W Y Z D V W X Y Z A B C D P Q R S T U V W X Y Z A B C D D D Q R S<!--</td--><td>A A B C D E F G H I J K L M N O P Q R S B B C D E F G H I J K L M N O P Q R S T U C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V E F G H I J K L M N O P Q R S T U V W F F G H I J K L M N O P Q R S T U V W G G H I J K L M N O P Q R S T U V W X Y G G H I J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B C D C D P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L W W X Y Z A B C D E F G H I J K L <td>A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C</td></td></td></td></td>	A A B C D E F G H I J K L M N O B B C D E F G H I J K L M N O P Q C C D E F G H I J K L M N O P Q R D D E F G H I J K L M N O P Q R S T U V </td <td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W N V N N P Q R S T U V W X Y Z A B C D R S T U V W X Y Z A B C D R S T U V W<!--</td--><td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R S T D D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W Y Z D V W Y Z D V W X Y Z A B C D P Q R S T U V W X Y Z A B C D D D Q R S<!--</td--><td>A A B C D E F G H I J K L M N O P Q R S B B C D E F G H I J K L M N O P Q R S T U C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V E F G H I J K L M N O P Q R S T U V W F F G H I J K L M N O P Q R S T U V W G G H I J K L M N O P Q R S T U V W X Y G G H I J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B C D C D P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L W W X Y Z A B C D E F G H I J K L <td>A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C</td></td></td></td>	A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W N V N N P Q R S T U V W X Y Z A B C D R S T U V W X Y Z A B C D R S T U V W </td <td>A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R S T D D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W Y Z D V W Y Z D V W X Y Z A B C D P Q R S T U V W X Y Z A B C D D D Q R S<!--</td--><td>A A B C D E F G H I J K L M N O P Q R S B B C D E F G H I J K L M N O P Q R S T U C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V E F G H I J K L M N O P Q R S T U V W F F G H I J K L M N O P Q R S T U V W G G H I J K L M N O P Q R S T U V W X Y G G H I J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B C D C D P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L W W X Y Z A B C D E F G H I J K L <td>A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C</td></td></td>	A A B C D E F G H I J K L M N O P Q R B B C D E F G H I J K L M N O P Q R S T D D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V W Y Z D V W Y Z D V W X Y Z A B C D P Q R S T U V W X Y Z A B C D D D Q R S </td <td>A A B C D E F G H I J K L M N O P Q R S B B C D E F G H I J K L M N O P Q R S T U C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V E F G H I J K L M N O P Q R S T U V W F F G H I J K L M N O P Q R S T U V W G G H I J K L M N O P Q R S T U V W X Y G G H I J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B C D C D P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L W W X Y Z A B C D E F G H I J K L <td>A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C</td></td>	A A B C D E F G H I J K L M N O P Q R S B B C D E F G H I J K L M N O P Q R S T U C C D E F G H I J K L M N O P Q R S T U D D E F G H I J K L M N O P Q R S T U V E F G H I J K L M N O P Q R S T U V W F F G H I J K L M N O P Q R S T U V W G G H I J K L M N O P Q R S T U V W X Y G G H I J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y J J K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B K K L M N O P Q R S T U V W X Y Z A B C D C D P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E M N N O P Q R S T U V W X Y Z A B C D E Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I Q Q R S T U V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L M V W X Y Z A B C D E F G H I J K L W W X Y Z A B C D E F G H I J K L <td>A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C</td>	A A B C D E F G H J K L M N O P Q R S T B B C D E F G H I J K L M N O P Q R S T U V C C D E F G H I J K L M N O P Q R S T U V W Z A B C	A A B C D E F G H I J K L M N O P Q R S T U V W B B C D E F G H I J K L M N O P Q R S T U V W X D D E F G H I K L M N O P Q R S T U V W Y Z A D D E F G H I J K L M N P Q R S T U W X Z A B C D D L M N D Q R S T U W X Z A B C D D L M N	A A B C D E F G H I J K L M N O P Q R S T U V W 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 D D E F G H I J K L M N O P Q R S T U 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 X Y Z A B C D D L L M N O P Q R S T U W X Z <td>A A B C D E F G H I J K L M N O P Q R S T U 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 W X Y Z A D D E F G H I K L M N O P Q R S T U W X Y Z A B C D E F G H I K L M N O P Q R S T U W X Z A B C D E G G H I J K L M N O P R S U W<td>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 B 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 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 C D E F G H I J K</td></td>	A A B C D E F G H I J K L M N O P Q R S T U 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 W X Y Z A D D E F G H I K L M N O P Q R S T U W X Y Z A B C D E F G H I K L M N O P Q R S T U W X Z A B C D E G G H I J K L M N O P R S U W <td>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 B 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 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 C D E F G H I J K</td>	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 B 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 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 C D E F G H I J K



- 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.



Example: "Playfair example"



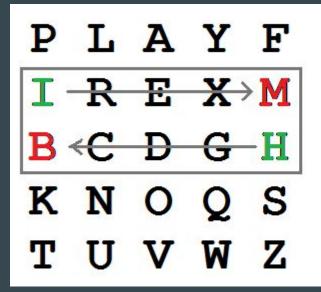


HI DE TH EG OL DI NT HE TR EX ES TU MP

X used to separate the repeated Es.



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



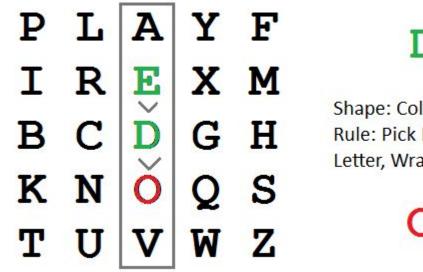
HI

Shape: Rectangle Rule: Pick Same Rows, Opposite Corners





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





Shape: Column Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD



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.

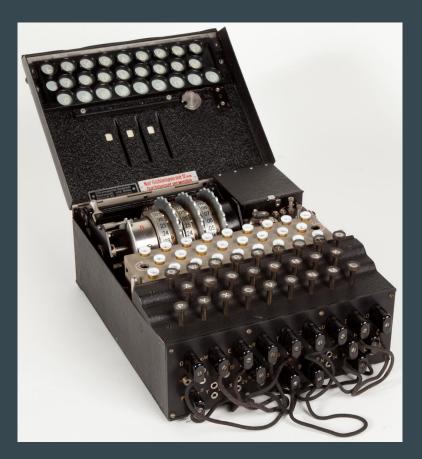
1885

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?

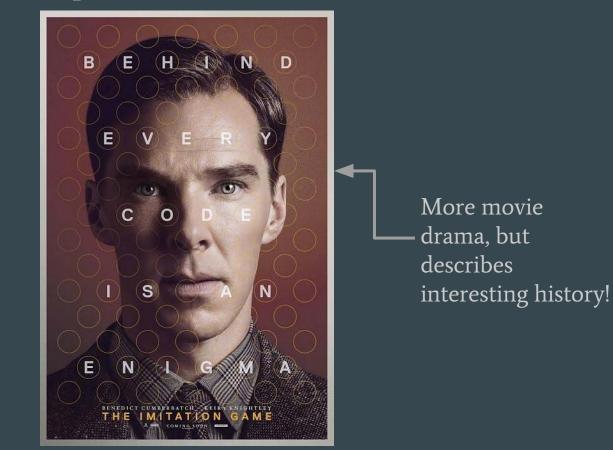
1920s

- 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



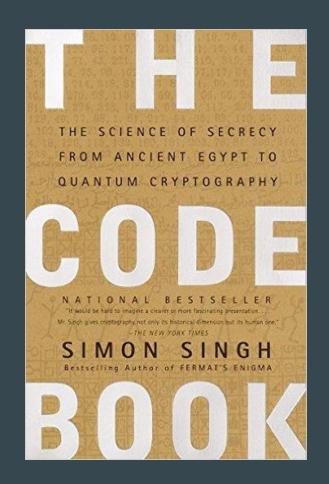
Recurring Theme (until the 1970s)

- 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).



This Course

What you'll learn:

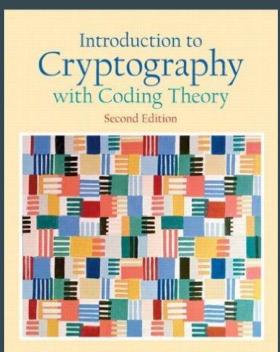
- Foundations and principles of the science
- Basic ingredients and components.
- Definitions and proofs of security
- High-level applications

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

Resources

- Course Website: <u>http://tigerweb.towson.edu/nmcnew/m314f17/</u>
- CoCalc: <u>http://www.cocalc.com/</u>
- The textbook:



Wade Trappe • Lawrence Washington