ARIZONA SCIENCE LAB

CIPHERS AND CODES

Keeping Information Safe

Institute Of Electrical And Electronic Engineers, Phoenix Section

Teacher In Service Program / Engineers In The Classroom (TISP/EIC)

"Helping Students Transfer What Is Learned In The Classroom To The World Beyond"

Our Sponsors

The AZ Science Lab is supported through very generous donations from corporations, non-profit organizations, and individuals, including:

Workshop Objectives

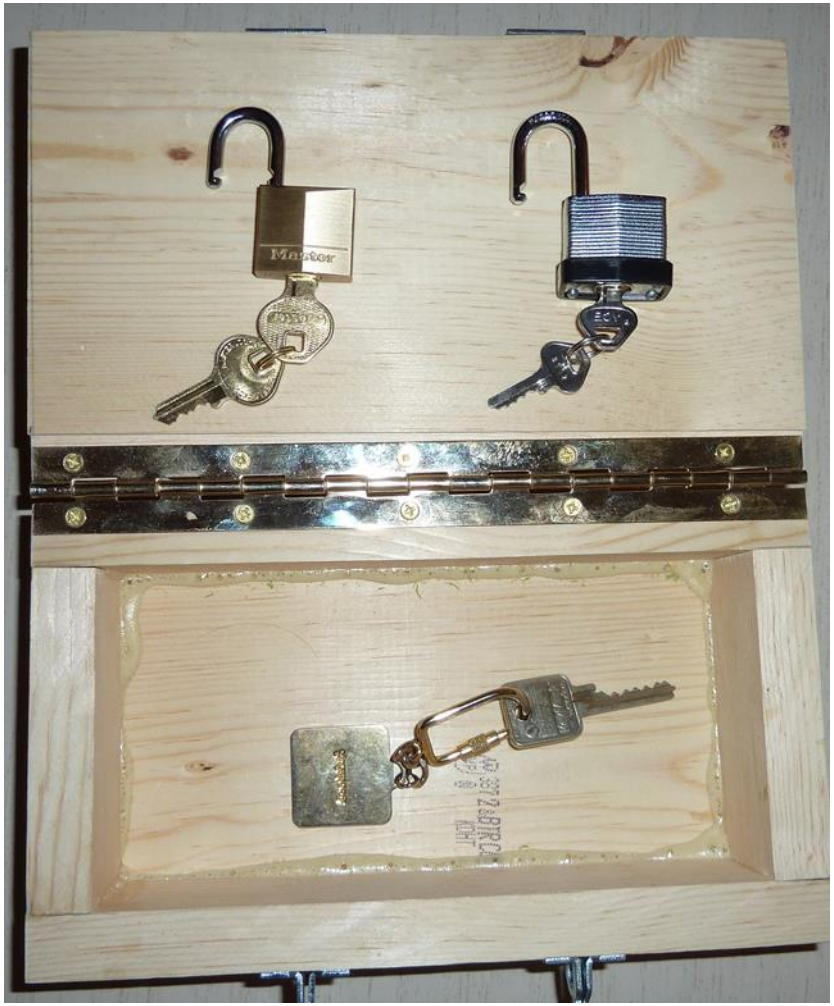
1. Learn about cryptography.
2. What are codes and ciphers?
3. See how they work.
4. Make and use some well-known ones!
5. AND have fun!


Protecting Information

Money Transfer Problem

- I want to send my friend $100.
- Some of my other “friends” promise to deliver it for me. I am not sure I trust them!
- I have a: box, two locks, each with a key.
- In planning for many transfers – I give one lock and its key to my friend.
- How do I make this transfer work via friends I cannot trust???

The box, locks, and keys



The importance of information today, the information age -

TV/Movies

amazon.com

MasterCard

On Line Purchases

Banking

Military communications

Business/personal information

E-mail

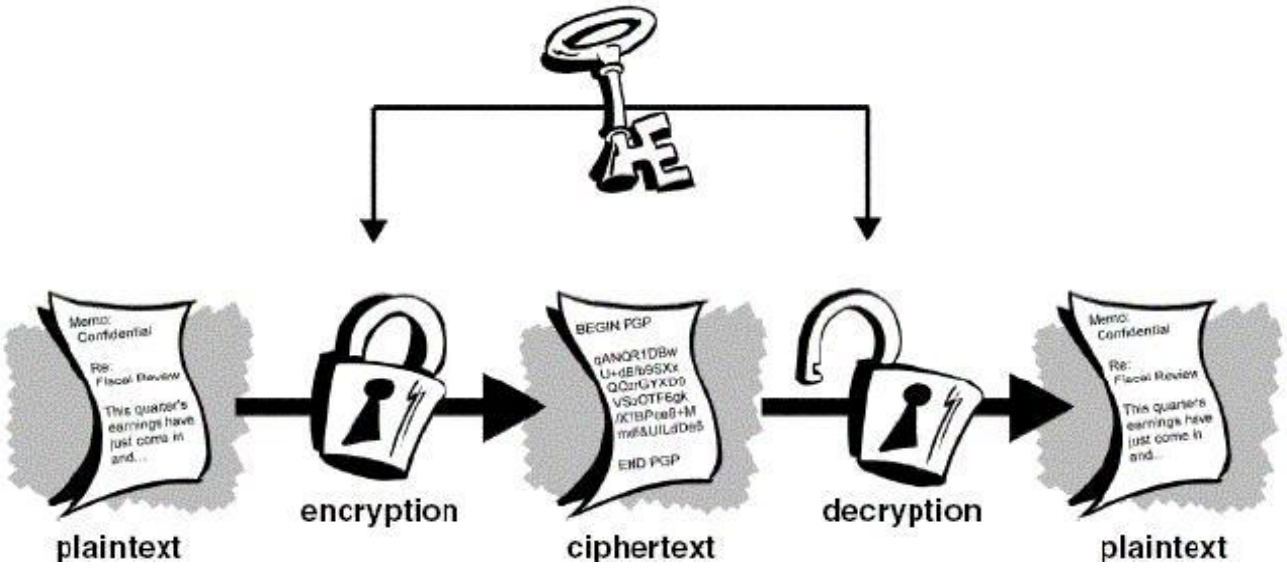
Protecting Information

As information is stored and transmitted we need to:

- Keep information private and confidential.
- Assure the information was not altered.
- Verify who sent or created the information.
- Validate that the sender did actually send the information.

Cryptography

- Greek: kryptos – hidden, graphein – to write
- The principles & techniques to encipher and decipher messages:



Some definitions

- Cipher – an algorithm (procedure or rule) used to disguise a message based on a key.
- Enciphering or encryption – process of scrambling a message to hide it.
- Key – the piece of information used by the cipher to create unique ciphertext.
- Code – a representation of a word, phrase, or message. May be secret or not.

Decryption

- Decrypting the message: recreating the original plaintext from the ciphertext.
- Always assume the ciphertext has been intercepted.
- AND – assume samples of plain and ciphertext are available to thief!
- Decryption is easy, knowing the cipher and the key!
- Decryption can be done by brute force or other techniques for weak ciphers.
- Good ciphers are very hard to break without knowing the key!

KEYS

Cryptographic Keys

The piece of information needed to unlock a cipher!

JOE
BOB

All of the ciphers in this next section use the same key for encryption and decryption – single key systems!

Transposition Cipher

- The characters in the plaintext are “shifted” according to a set of rules governed by the “key”.
- In many, the text is written down as a grid or table: m–columns x n–rows (either fixed or driven by the “key”).
- Then it is read out either fixed or according to the “key”.
- Ex: column cipher – write out message in rows, each the length of the key, the key sets: readout column order. Can either fill blanks with anything or skip blanks.

Key = “zebras” (632415) Plaintext = WE ARE DISCOVERED FLEE NOW

```
6 3 2 4 1 5

W E A R E D
I S C O V E
R E D F L E
E N O W
```

“EVLACDOESENROFWDEEWIRE”

Exercise: Decipher a message

- Cryptoanalysis: breaking a cipher
- Without the key, use clues:
  - who sent the message
  - frequency count of characters
  - other clues

Decrypt this (see activity sheet):

WTANEOZCL ECTS OHCLMEIAE EB

A Hint

This is a rectangular transposition cipher (rows and columns) – the text has been scrambled but the letters have not been changed:

WTANEOZCL ECTS OHCLMEIAE EB

WTAN|EOZC|L E|CTS |OHCL|MEIA|E EB

Transposition Cipher

WTAN | EOZC | L E | CTS | OHCL | MEIA | E EB

W	T	A	N
E	O	Z	C
L			E
C	T	S	
O	H	C	L
M	E	I	A
E		E	B

Key = 4

Codes

- A representation of a symbol, word, phrase, or message.
- Codes can keep messages short or easy to use:
  - Alphabet to numbers -> ASCII code: A=65; B=66;…
  - Police -> 10-4: understood; 10-0: use caution
  - Morse code - > dots, dashes, spaces: light, radio, wired network
  - You use emoticons during texting: ☺ or : -)
- Codes can be public or used to keep messages secret!

Morse Code

Morse code: transmitting information, using short and long marks or pulses - "dots" and "dashes" - for the letters, numerals, punctuation of a message. It was created by Friedrich Clemens Gerke for Samuel Morse's (1791-1872) electric telegraph in 1848, and is used primarily in radio communication.

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

Morse code sent at 5 words per minute:

TEXT IS FROM AUGUST 2008 QST Pages 36 and 89

_ • _•• _ •• ••• ••_• •_• ___ __ •_ ••_ __• ••_ ••• _

T E X T I S F R O M A U G U S T

Morse code sent at 20 words per minute:

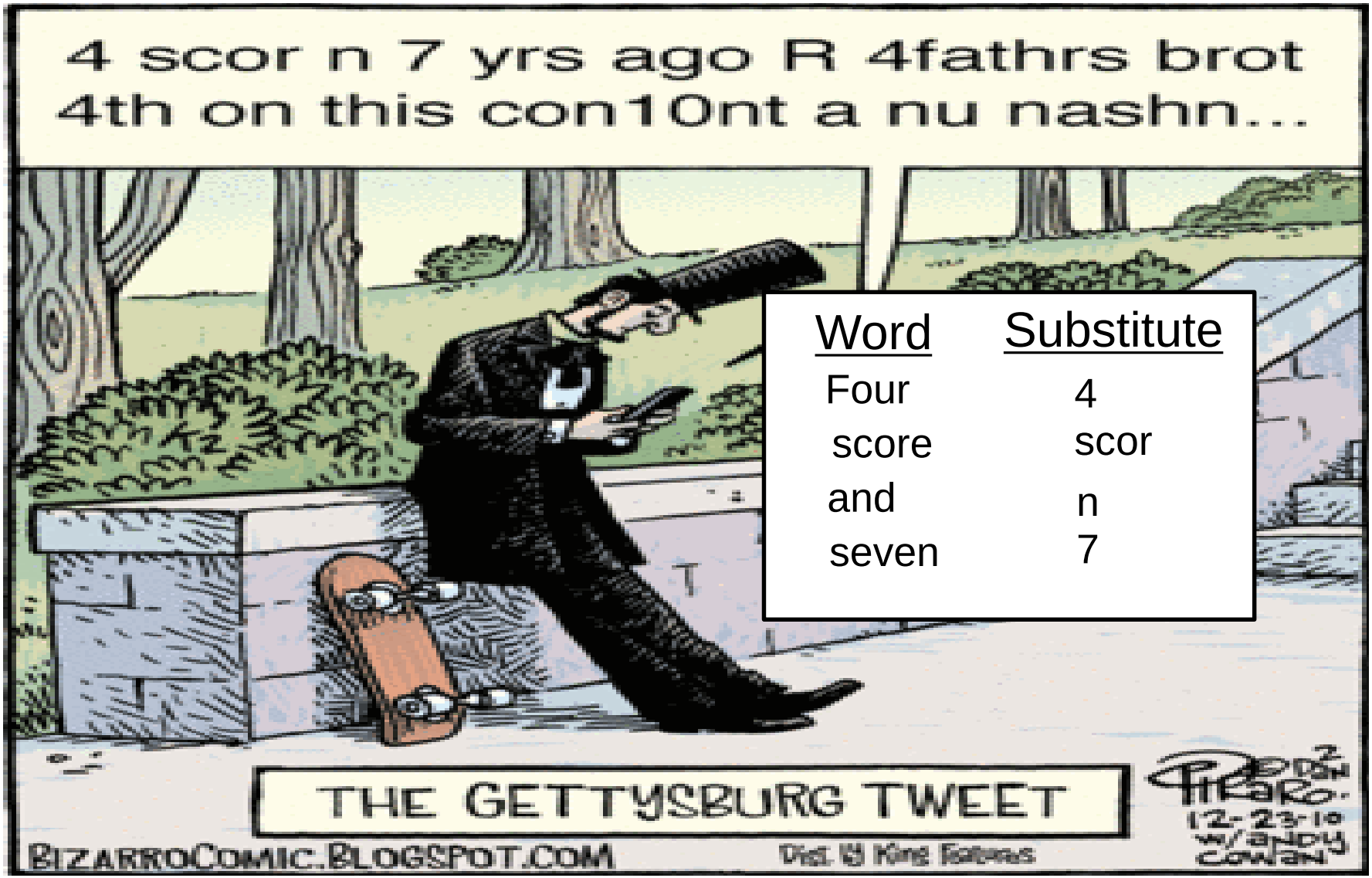
TEXT IS FROM MARCH 2009 QST PAGES 70 and 71

COMMONLY ENCOUNTERED REQUIREMENTS FOR MOST AMATEURS. THERE ARE LIMITS FOR ALL FREQUENCIES, SO FOR OTHER FREQUENCY RANGES, LOOK IN THE PREVIOUSLY CITED REFERENCES. THE BASIC PROCESS IS TO ENSURE THAT THE EXPOSURE TO HUMANS FROM YOUR ANTENNA SYSTEM, OR ANY OTHER PART OF YOUR STATION, DOES NOT EXCEED THE LIMITS.

Morse code sent at 40 words per minute:

TEXT IS FROM AUGUST 2009 QST PAGES 69 and 70

Codes: *Substitute* and *Swap* Letters, Numbers, Symbols



Word	Substitute
Four	4
score	scor
and	n
seven	7

History of Ciphers

- Ciphers have been used since the beginning of written text.
- Spartans in Greece – 2000 years ago (scytale)
- Romans – Julius Caesar (Caesar – shift cipher)
- WWII (Enigma)
- Modern codes: DES, RSA.

US Government

The US government agency responsible for cybersecurity is:

NSA – National Security Agency

check out their kids bio website:

https://www.nsa.gov/kids/home.shtml

Key Transmission

For the ciphers that follow:

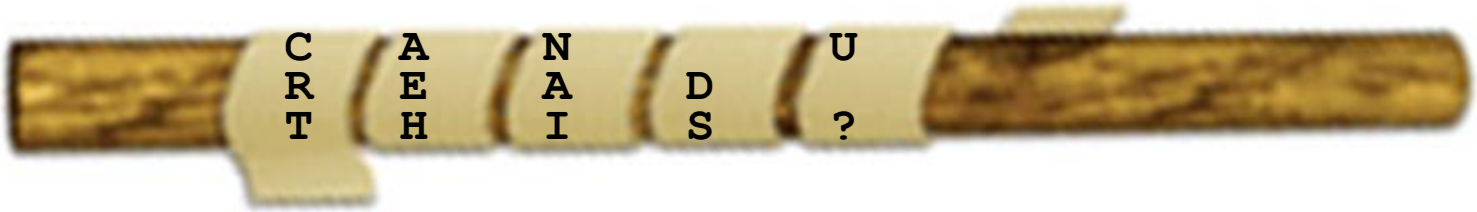
The single key used for encryption and decryption must be securely transmitted between the sender and the receiver before it can be used to send secret information.

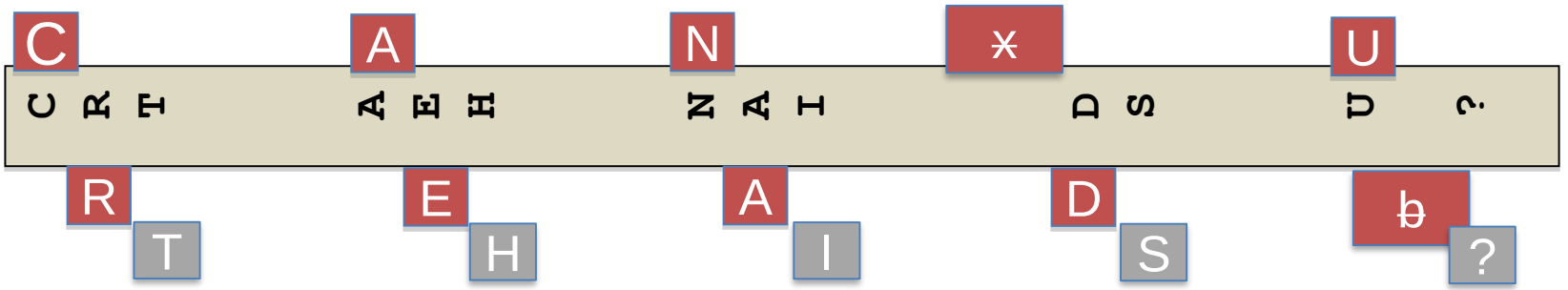
This can be an issue!

SCYTALE (Pronounced skit' il lee)

Spartan messengers carried coded messages on their belts: it is a transposition cipher

SCYTALE Example





C A N U R E A D T H I S ?

Key = ??

Exercise: EXCHANGE SCYTALE MESSAGES

Step 1. Wind the scytale strip on the rod and tape it at both ends.

Step 2. Think up your own short message to send to your partner, (example: “I like the shirt you are wearing” or “I have a lot of homework tonight”), and write it on the line on the activity sheet and on the mounted Scytale strip.

Step 3. Unwind one end (only!) of the scytale strip and exchange the rod with your partner’s.

Step 4. Try to read the unwound message.

Step 5. Wind your partner’s scytale strip on its rod, read the message, and write it in the line on the activity sheet.

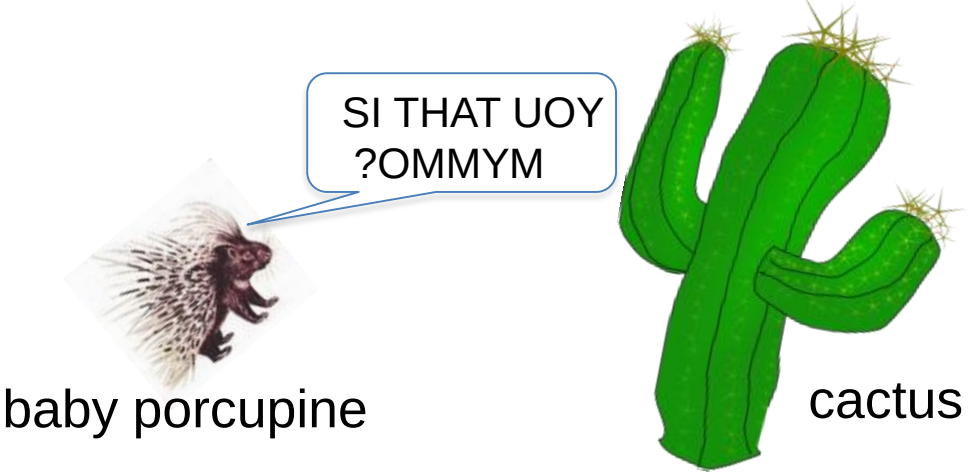
More Transposition Ciphers:

Substitute and *Swap* Letters, Numbers, Symbols

What did the baby porcupine ask the cactus?

(Coded) Answer:

SI TAHT UOY ?YMMOM

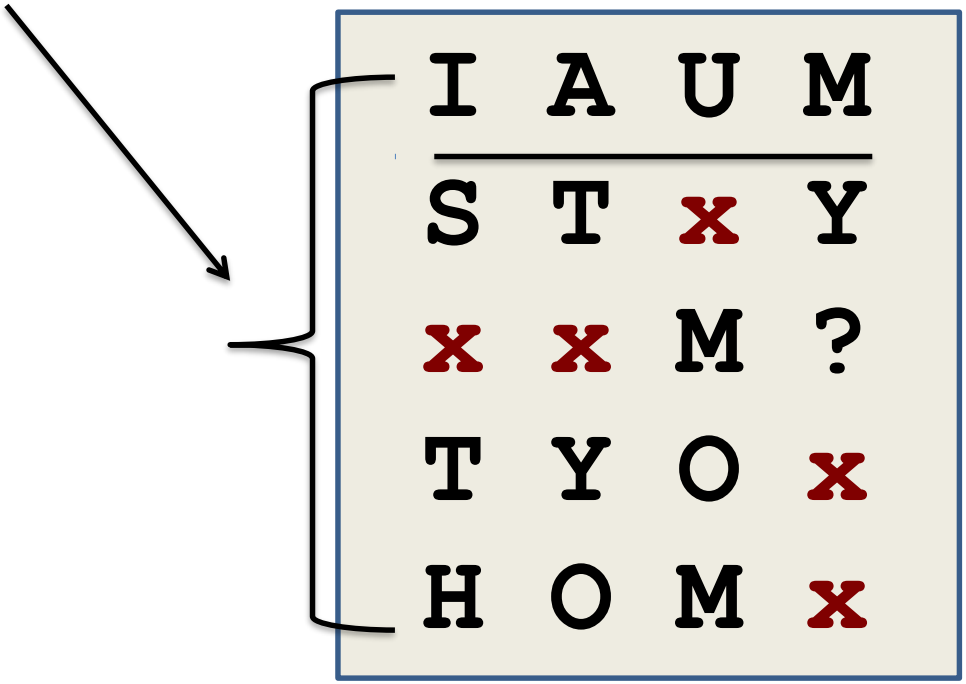


Decoded Answer:

IS THAT YOU MOMMY?

Solution Using A Rectangular Transposition Cipher

/ISxTH/ATxYO/UxMOM/MY?xx/



I	A	U	M
S	T	x	Y
x	x	M	?
T	Y	O	x
H	O	M	x

Key - ??

IAUM STxY xxM? TYOx HOMx

Other Rearrangements

ISxTHATxYOUxMOMMY?xx

Some possibilities:

xx?YMMOMxUOYxTAHTxSI (backwards)

xxMOMMY?xYOUxTHATxIS (reversed words)

Exercise: Student Rearrangements

Make up your own rearrangement of

ISxTHATxYOUxMOMMY?xx

(keeping the words together) and write it in the space on the Activity Sheet.

Can you decode this??

Random Order

Randomly selecting the letters:

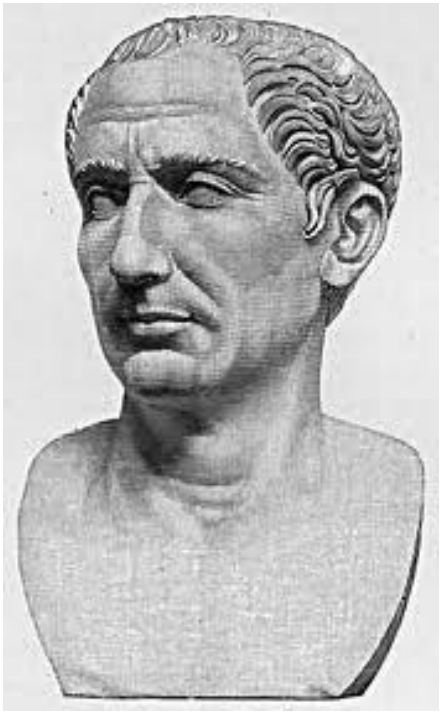
Y M x x x x A? T T O I H S U O Y M M

Remember: ciphers only work if they can be decrypted by someone who has the “key”. The “key” can be explicit or in the cipher algorithm.

Substitution Ciphers

- Can be very secure depending on the complexity of the substitutions.
- The deciphering of simple uniform substitutions can be assisted by character frequency distribution and context.
- Complex substitutions that hide frequency distributions are more difficult to decrypt.
- The larger the key value range the better!

Caesar Wheel



Julius Caesar (100-45 BC)

A monoalphabetic substitution cipher

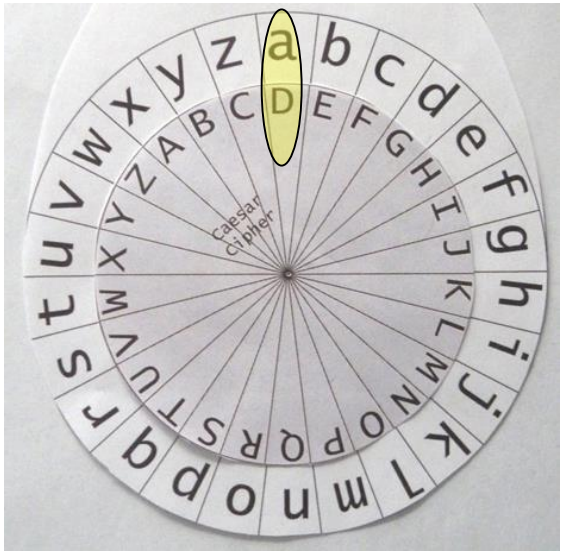
The Caesar (Shift) Cipher

Caesar used a "shift code" with a "Key=3" for messages to his Generals.

Key = 3

a is replaced by **D**
b is replaced by **E**
c is replaced by **F**
...
y is replaced by **B**
z is replaced by **C**

meet me Dt seven
Dt mcdonDlds



Caesar's Code (continued)

meet me at seven at mcdonalds

PHHW PH W H H W P

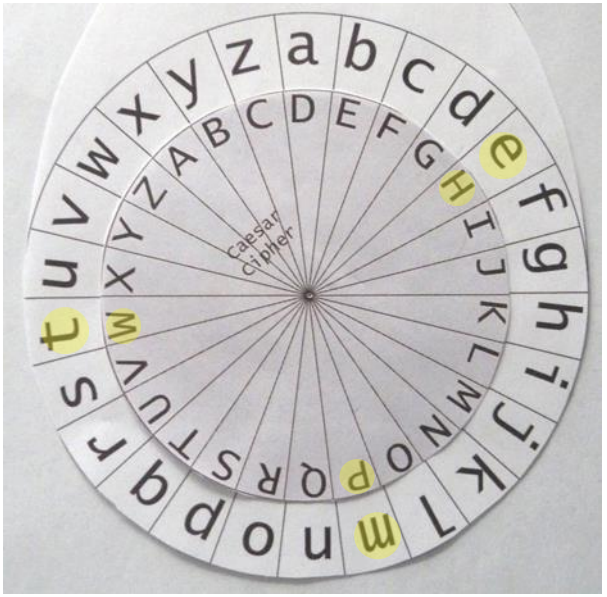
PHHW PH DW VHYHQ DW PFGRQDOGV

key = 3

m becomes P

e becomes H

t becomes W



Other Values Of The Key

Key = 3 is the value that Caesar used:

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
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

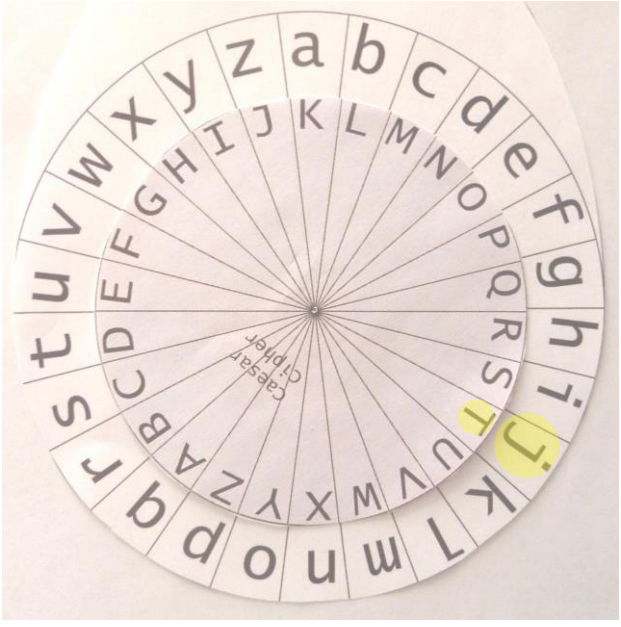
If Key = 10, what does “j” code to?

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
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

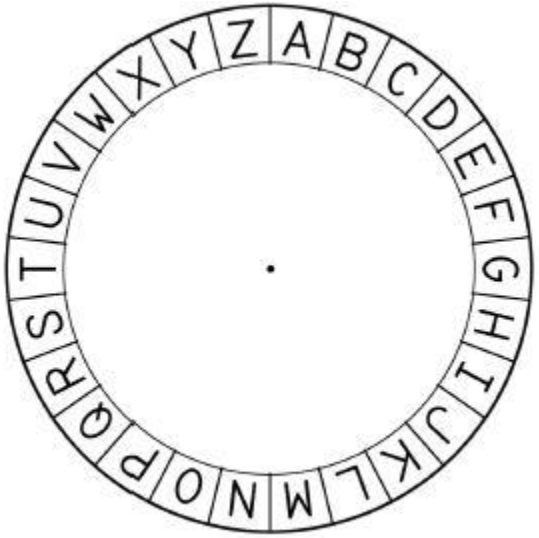
How many values can Key have?

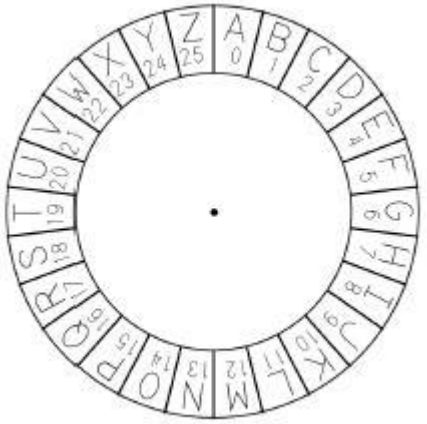
26: 0, 1, 2, 3, … ,25

Is that good??



Exercise: Construct A Caesar Wheel





1. **Cut out the large "Plain Text" Cipher Wheel and the smaller "Caesar Cipher" wheel on the Handout.**

2. **Using the brass fastener, push it through the center of the Caesar Cipher wheel, then carefully push this through the Plain Text wheel. Open the tabs to fasten.**

3. **You have a Caesar Substitution Cipher Wheel!!!**

Exercise (continued)

Try out your Caesar Wheel on the coded text:

H P H T W W X P P E L E X T O Y T R S E

(The Key is NOT 3. It is between 9 and 12.)

The Key is 11.
The decoded message is:

WE WILL MEET AT MIDNIGHT

Website for coding/decoding software:

http://www.braingle.com/brainteasers/codes/caesar.php

Exercise: Caesar-Wheel Message Exchange

For a (short!) secret message of your choosing,

1. Code the message with a Key of your choosing.

2. Exchange the coded message with a partner.
   (First don't tell each other what your key is, then give it to your partner).

3. Decode your partner's message.

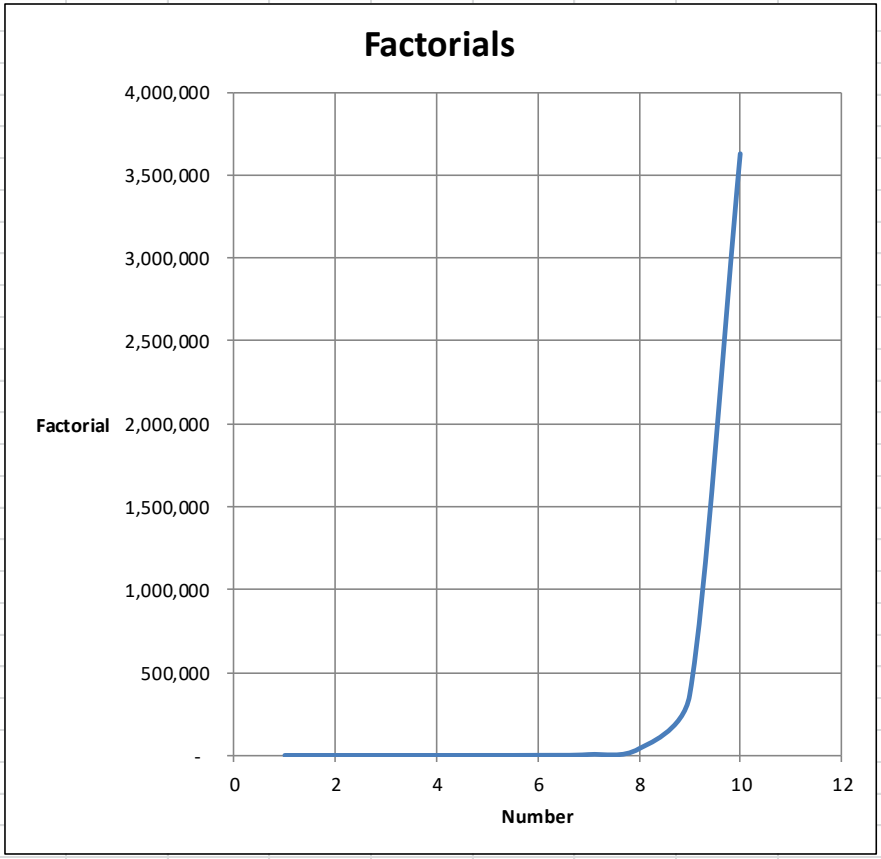
Key Length

- The shift substitution cipher is limited to 26 keys – breaking this is pretty easy!
- An alternative:
  - Mixed Alphabet Cipher: the ciphertext alphabet is created using an "alphabetic key" rather than a simple 1-26 number.
  - Pick a key (word or phrase), write it down using letters only once, then finish with rest of the alphabet. The longer the key the better!

Mixed Alphabet Cipher

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

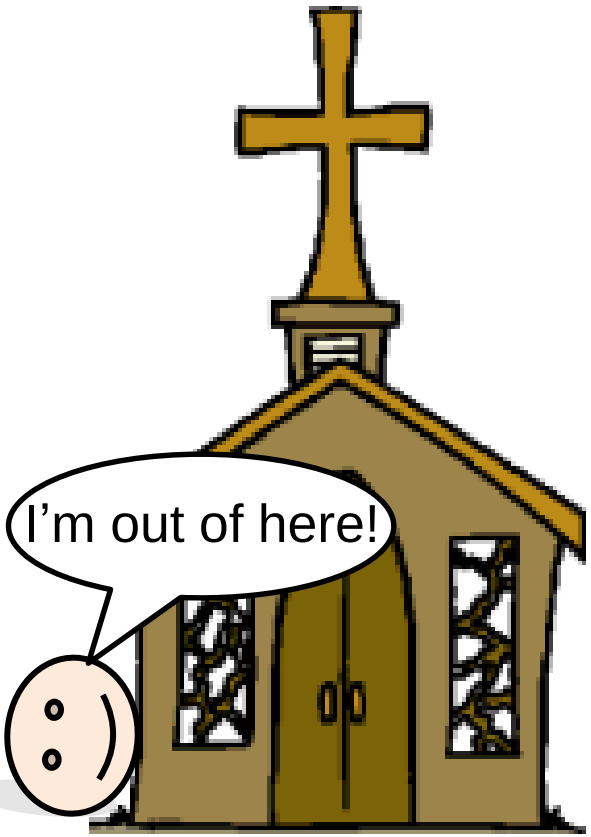
Number	Factorial
1	1
2	2
3	6
4	24
5	120
6	720
7	5,040
8	40,320
9	362,880
10	3,628,800
11	39,916,800
12	479,001,600
13	6,227,020,800
14	87,178,291,200
15	1,307,674,368,000
16	20,922,789,888,000
17	355,687,428,096,000
18	6,402,373,705,728,000
19	121,645,100,408,832,000
20	2,432,902,008,176,640,000
21	51,090,942,171,709,400,000
22	1,124,000,727,777,610,000,000
23	25,852,016,738,885,000,000,000
24	620,448,401,733,239,000,000,000
25	15,511,210,043,331,000,000,000,000
26	403,291,461,126,606,000,000,000,000
	403 Septillion!



Null Cipher

- Hide the message within a much longer text message of no meaning.
- Use clues to locate the characters of the message, i.e. newspaper classifieds titles.
- Next exercise: every 3rd character after a punctuation mark is part of the message!

Exercise: Secret Message, Sliding Panel



Chapel

Worthie Sir John: Hope, that is the beste
comfo I
fear y to
you, le to
requi
askin what
I can do, bee very sure I will. I knowe
that, ear
it, it frights not you, accounting it for a
high honour to have such a reward of your
soe bitter, cup. I fear not that you
of a wise man. Tell me, an if you can,
for you anything that you wolde have
done. The general goes back on Wednesday.
Restinge your servant to command.
[Signed] R.T.

Complete Hidden Message Activity to find the hidden message.

pa

panelateastendofchapelslides

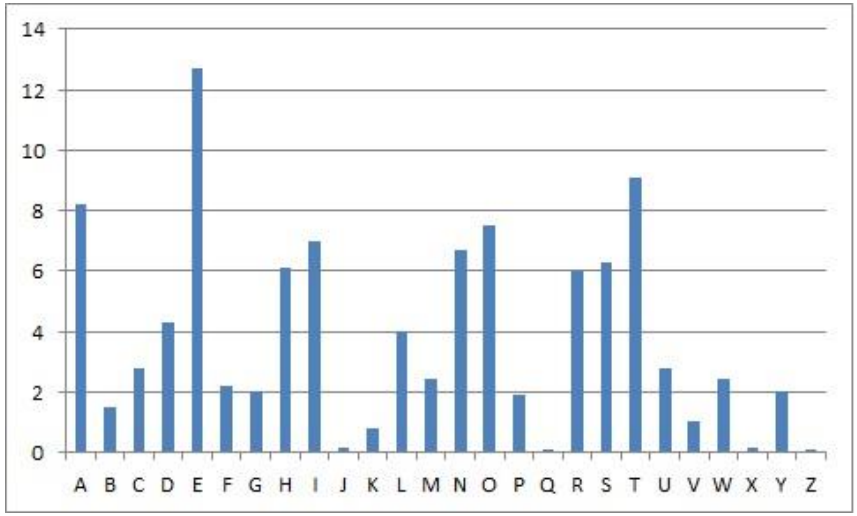
anel at east end of chapel slides

Techniques: Frequency Analysis

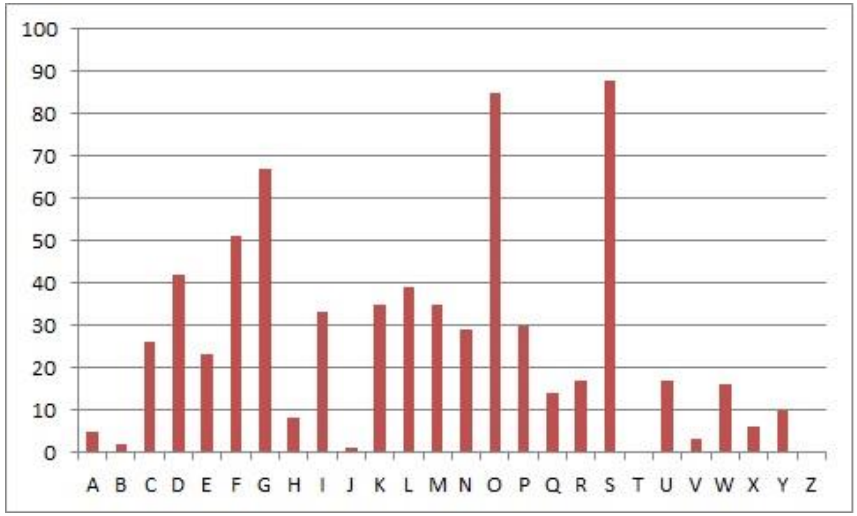
- In a monoalphabetic substitution cipher:
  - Even with substitutions, the frequency of letters remains the same: ex: e -> p
  - We disguise the letters, but patterns remain!
  - Ex: The lazy dog jumped over the fence.
  - The 5 e's just become 5 of another letter!
  - Using frequency analysis and patterns we can find such words as: the, as, by, … and then the whole message!!!

English Frequency Table

Letter	Frequency
e	12.7
t	9.1
a	8.2
o	7.5
i	7.0
n	6.7
s	6.3
h	6.1
r	6.0
d	4.3
l	4.0
c	2.8
u	2.8
m	2.4
w	2.4
f	2.2
g	2.0
y	2.0
p	1.9
b	1.5
v	1.0
k	0.8
j	0.15
x	0.15
q	0.10
z	0.07



Plaintext



Ciphertext

Polyalphabetic Cipher

- A substitution cipher, but the cipher alphabet changes during the process – reduces the frequency of letters issue.
- Vigenère cipher developed in 1585.
- Widely used and more difficult to break than simple mono substitution.
- Each letter in the keyword determines the next substitution. The longer the keyword the more secure.

Vigenère Cipher

	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

Using the Vigenere Cipher

- Pick a “keyword” and write down under plaintext, repeat keyword to end of text.
- Look up keyword letter “row”, find plaintext “letter”, go up to ciphertext.
- The keyword letter sets the shift amount, like Caesar code, but it changes with every letter!

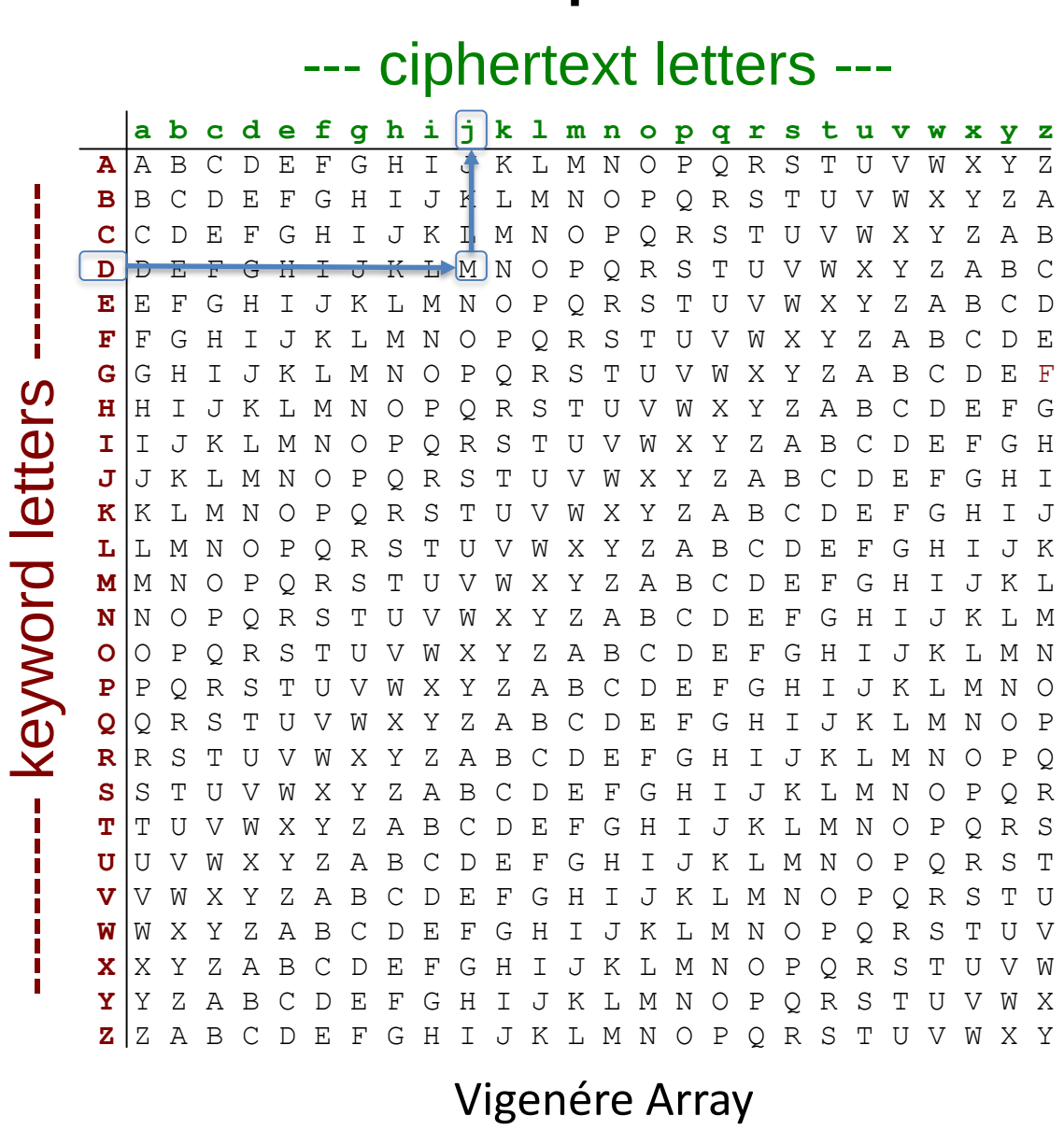
How To Use The Cipher

1. Find the keyword letter in the left-most column.
2. Move in to the plaintext letter.
3. Move up to the ciphertext letter.

MY MESSAGE - plaintext
DO GDOGDOG – key

jk gbemxsy – ciphertext
do gdogdog - key

MY MESSAGE - plaintext



Vigenére Array

Exercise: V Cipher Message Exchange

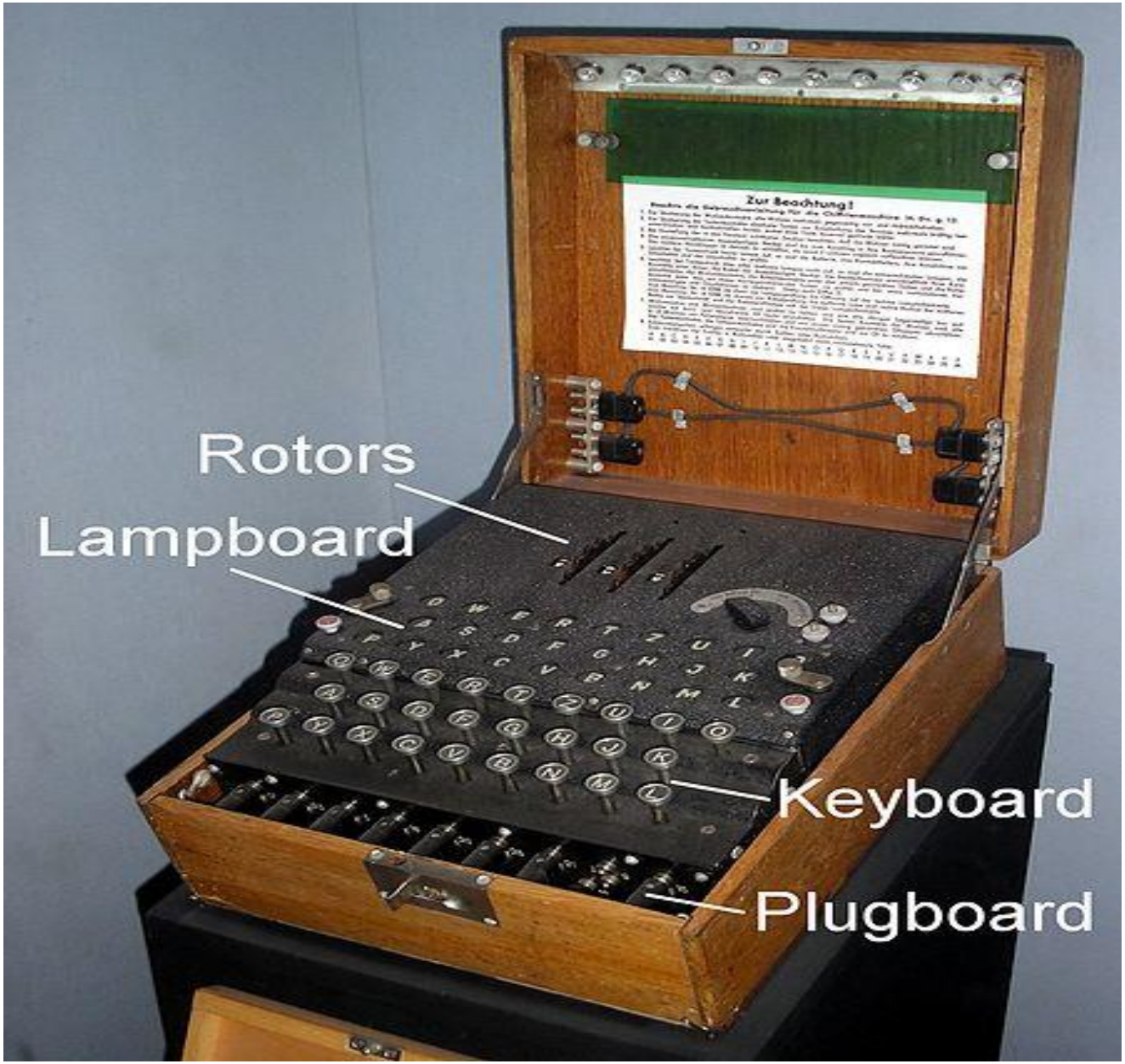
For a (short) secret message of your choice:

1. Code the message with a Vigenère Cipher.
2. Exchange the message with that of a partner.
3. Decode your partner's message. (Please tell each other the Keyword you used)

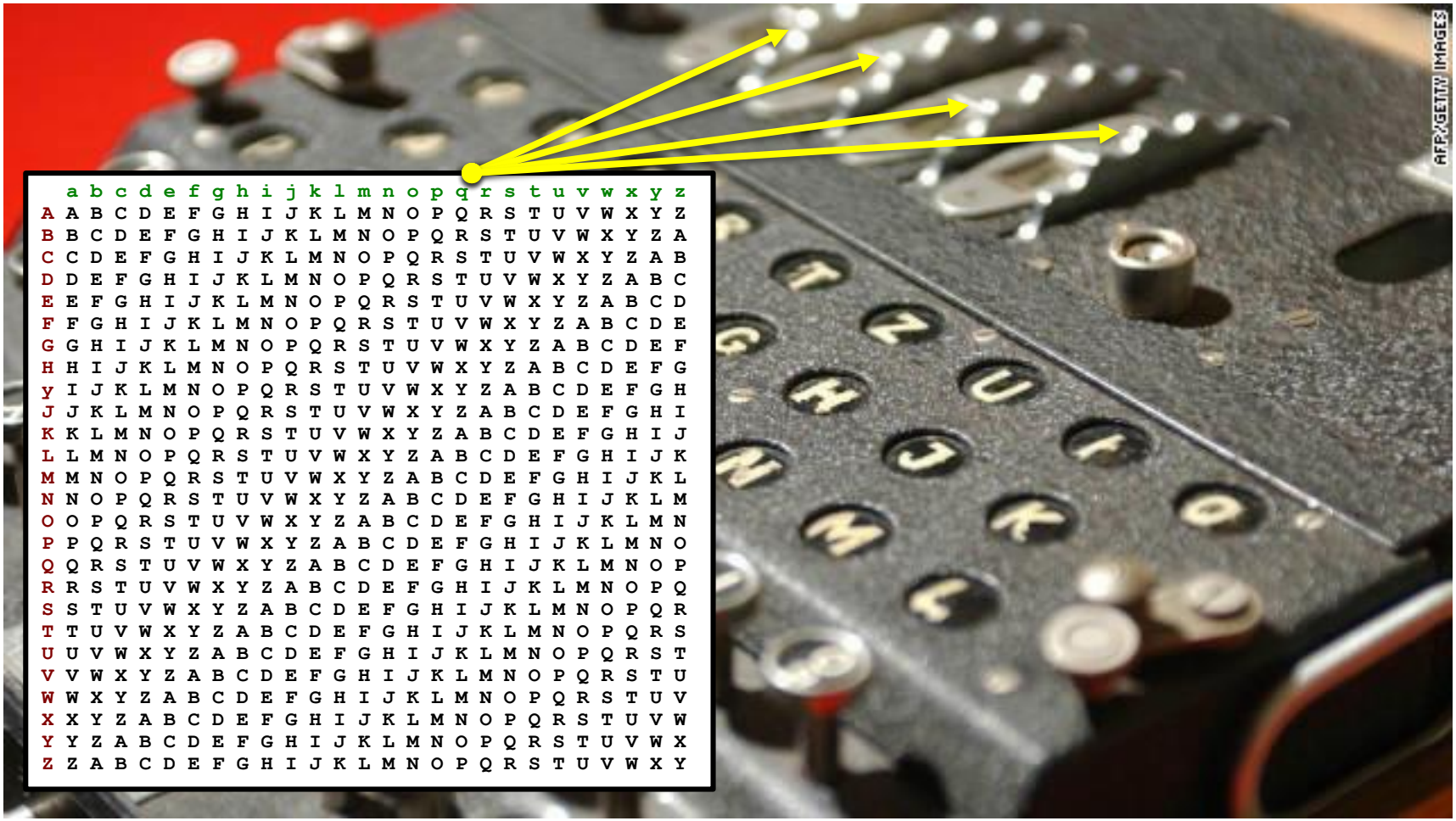
Enigma Coding Machine

This German coding system, used by its Navy, was the best one before computers were invented.

The code was broken by the British and the Americans even before the U.S. entered the war.



Enigma Machine



	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
y	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

After multiple rotations, the rotor positions yield the proper shifted alphabet for determining the coded (or decoded) letter.

Decrypting Enigma Messages

- The original Enigma machine was invented by a German electrical engineer, Arthur Scherbius.
- Alan Turing, an English mathematician, and his team built a device called the Bombe which could decode Enigma messages fairly quickly.

Bletchley Park, England

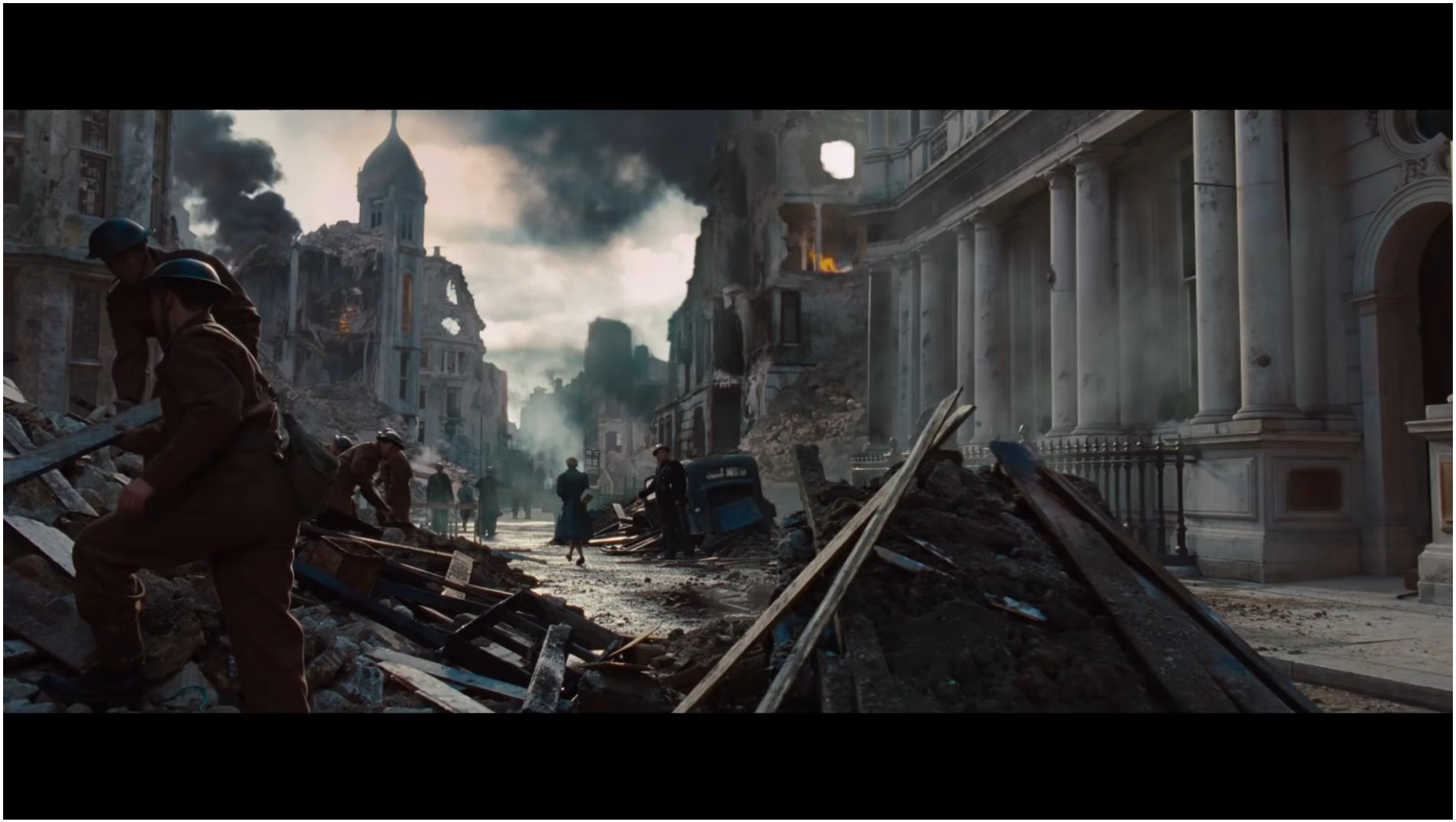
Bletchley Park built 16 machines to crack the Enigma code.

These were used day and night to decipher Enigma messages sent by the German Navy.

By early 1942 the British were able to decipher all that day's messages within an hour.

The Enigma Movie

The Imitation Game



Summary:
Cipher Techniques We Discussed So Far

1. Transposition
2. Substitution
3. Null
4. Coding
5. Scytale
6. Caesar Shift
7. Vigenère
8. Enigma Machine

ALL OF THESE ARE DEPENDENT ON THE SENDER AND RECEIVER HAVING EXCHANGED A SECRET "KEY"

Breaking the Code

- We always assume:
  - The Spy has some samples of plaintext/ciphertext combinations.
  - The Spy knows the cipher algorithm, but not the key.
  - Still cannot find key or decrypt messages.
  - Modern computers make trial and error very very easy.
  - We need more complex algorithms.

Key Management

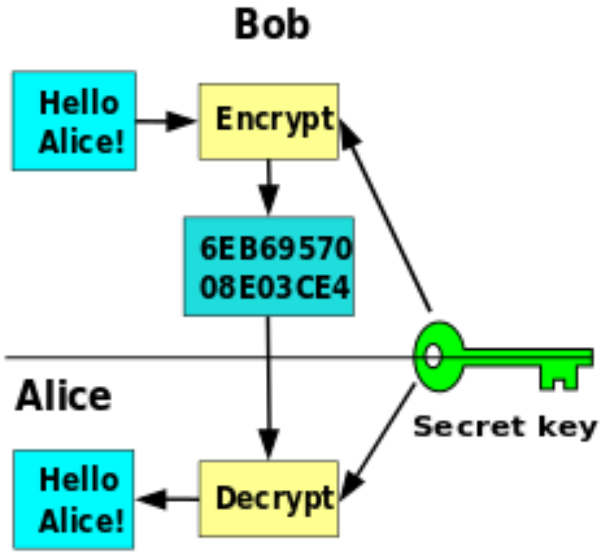
- All of the techniques we have discussed use a “symmetric” or the same single key.
- It must be kept private for the cipher to work –> to keep the messages secret!
- Keys must be sent secretly to the receiver.
- Does not prevent forgery of messages: (creating a false message claiming sent by sender).
- A newer technique uses a “pair” of keys:

  Asymmetric keys – one public and one private

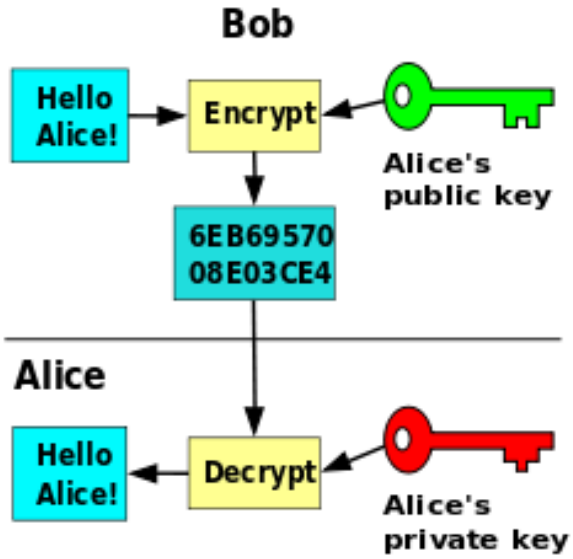
Public-Key Cryptography

- Probably the most significant advance in the 3000 year history of cryptography.
- Uses **two** keys – a public & a private key.
- **Asymmetric** since parties are **not** equal.
- One party is the message sender and one the receiver.
- Complements **rather than** replaces private key cryptography.

Two Keys



Single Key Cryptography



Two Key Cryptography

Asymmetric Keys

- Two keys – related but you cannot discover one from the other!
- These keys are created through a mathematical algorithm involving very large prime numbers.
- It is a very very difficult problem:
  - Given a very large number (100's of digits) that is the product of two very large prime numbers, to discover (factor the number) into those two prime numbers:

$$C = A * B$$

Prime Numbers

- prime numbers only have divisors of 1 and itself:
  - they cannot be written as a product of other numbers
  - note: 1 is prime, but is generally not of interest
- eg. 2,3,5,7 are prime, 4,6,8,9,10 are not
- list of prime number less than 200 is:

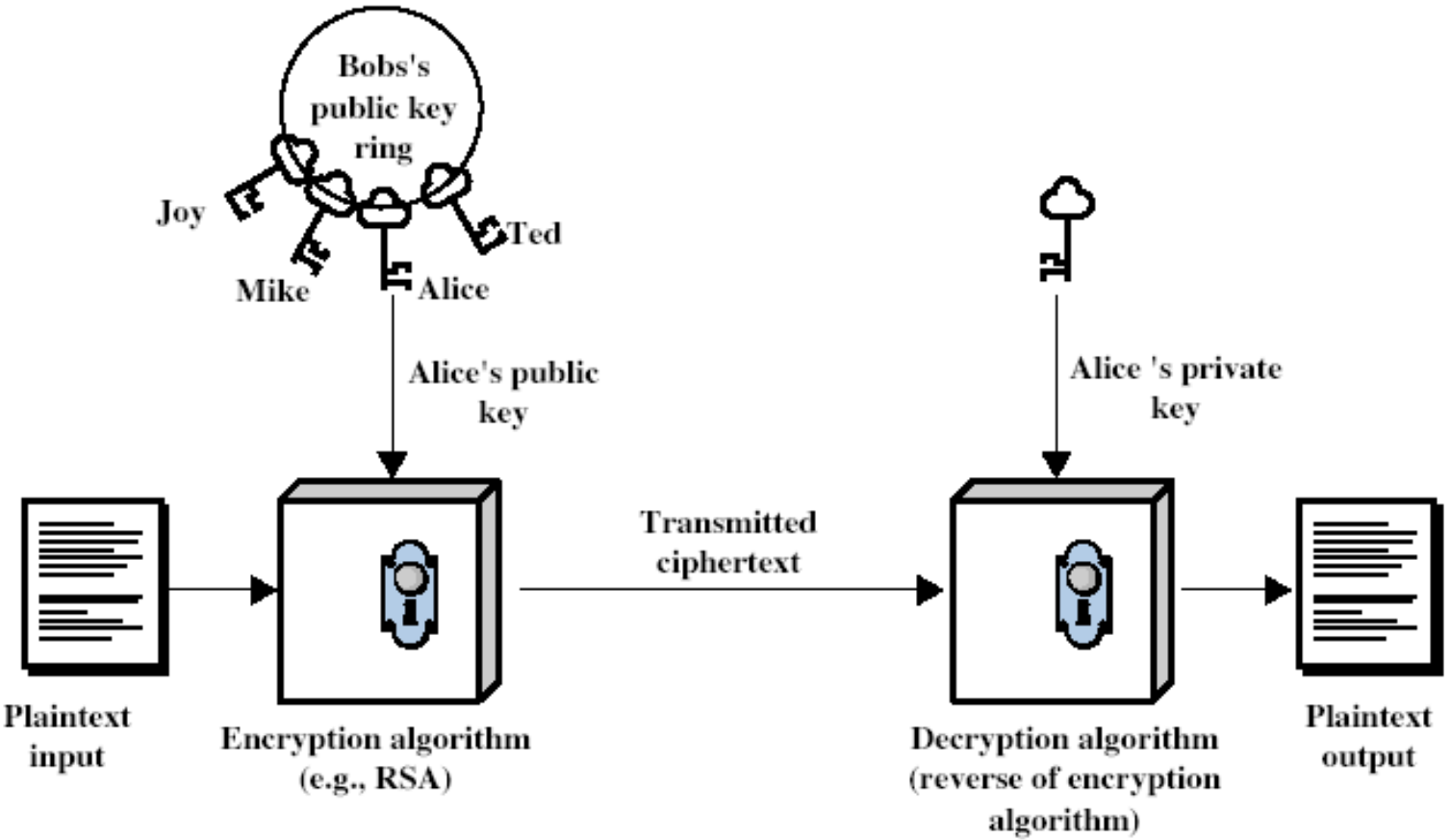
```
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67
71 73 79 83 89 97 101 103 107 109 113 127 131 137 139
  149 151 157 163 167 173 179 181 191 193 197 199
```

Public Key Cryptography

- **Public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**
- It is **asymmetric** because:

  those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

Public Key Cryptography



Why Public-Key Cryptography?

- Developed to address two key issues:
  - **key distribution** – how to have secure communications in general without having to trust a Key Dist. Center with your key.
  - **digital signatures** – how to verify a message comes intact from the claimed sender.
- Public invention due to Whitfield Diffie & Martin Hellman at Stanford University in 1976.

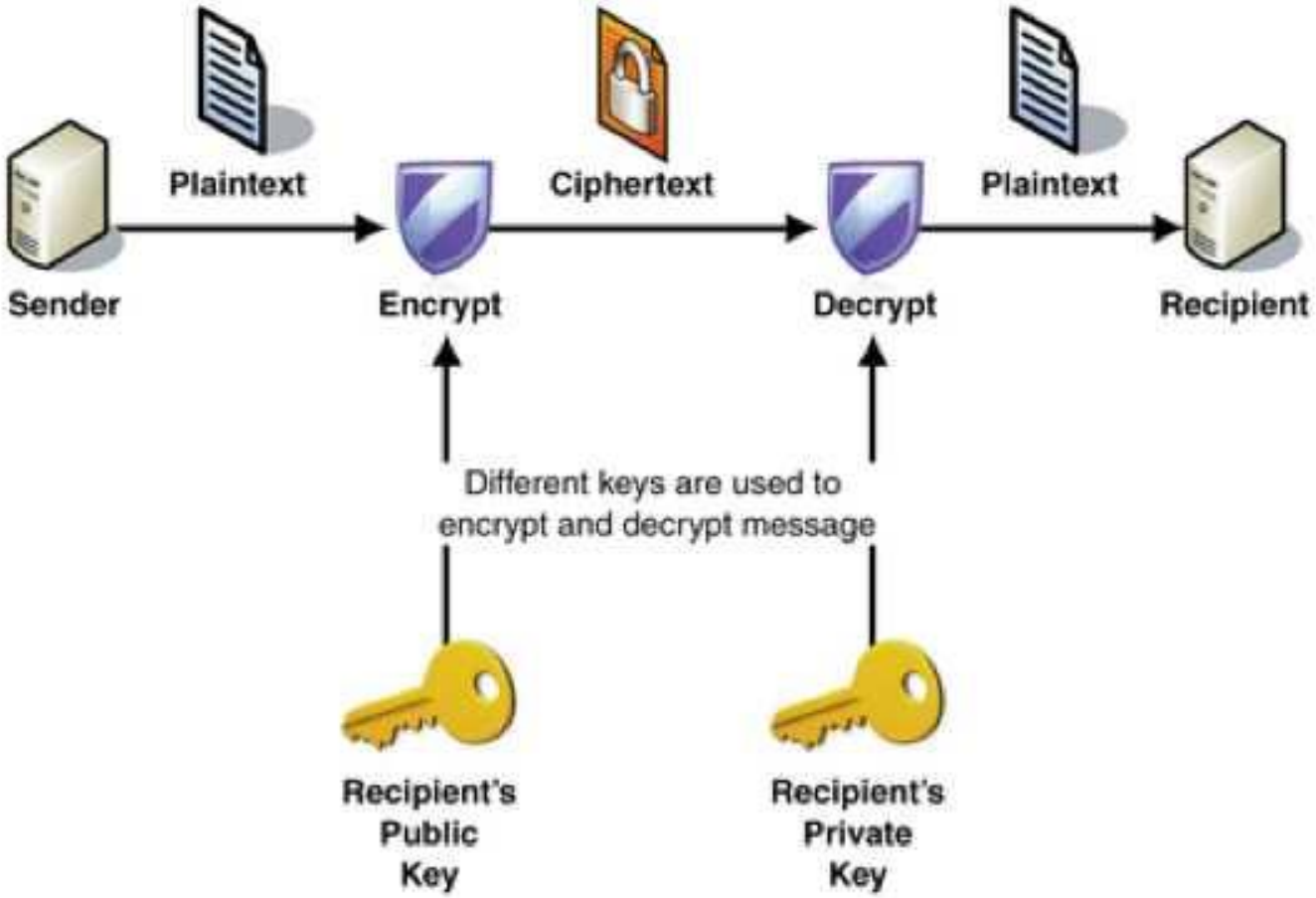
R S A

- Currently used public-key cryptosystem
- Created by Rivest, Shamir & Adleman from MIT in 1977
- Uses large integers (eg. 1024 bits)
- Highly secure due to cost of factoring very large numbers.

Prime Factorization

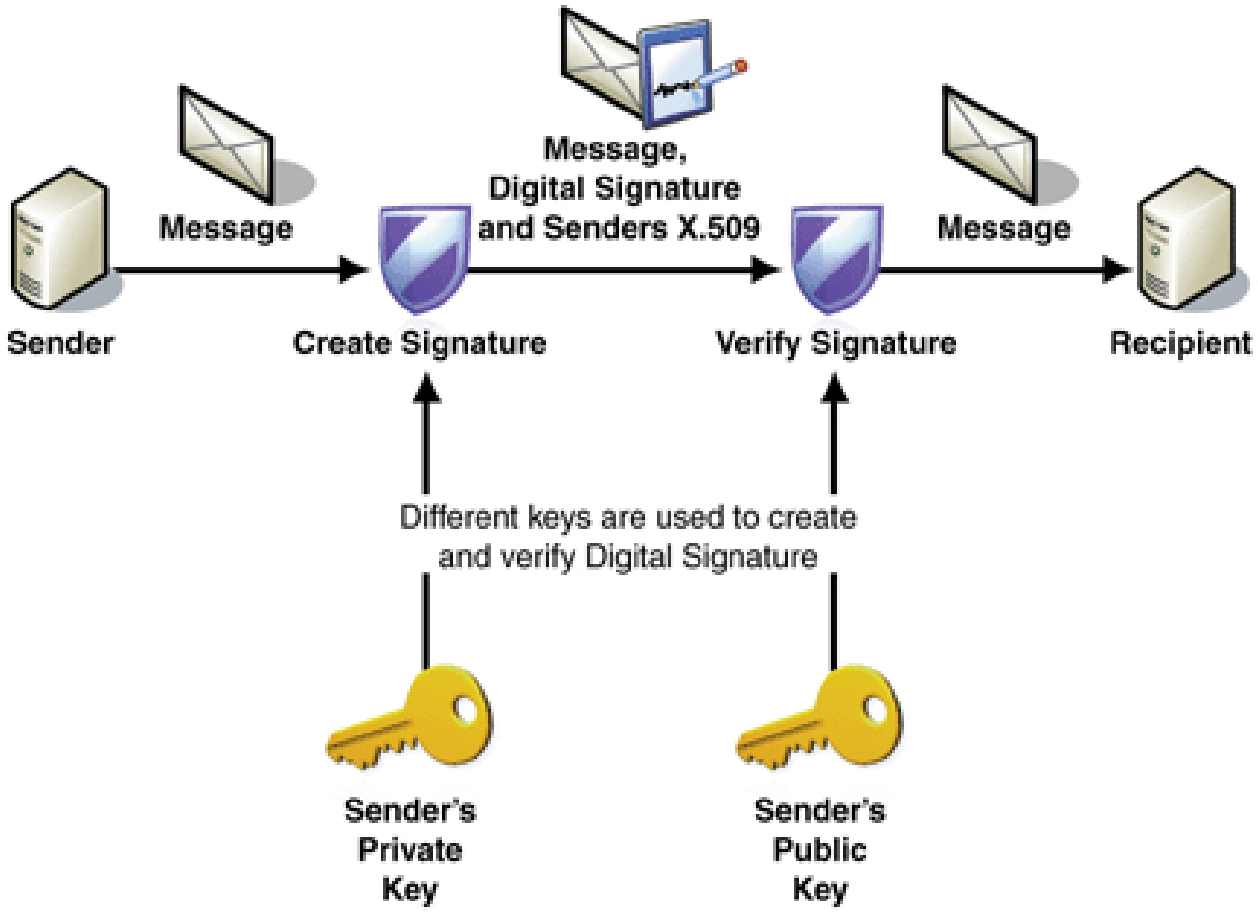
- to **factor** a number n is to write it as a product of other numbers: $n=a \times b \times c$
- note that factoring a number is relatively hard compared to multiplying the factors together to generate the number.
- the **prime factorization** of a number n is when its written as a product of primes
  - eg. $91=7\times13$; $3600=2^4\times3^2\times5^2$

Asymmetric Key System



Digital Signatures:

Use the two keys in reverse!



Project: A Murder Mystery

The Workshop Project

You will work in teams of 6 (your table)

Your job is to decode the clues to find:

1. the identity of **the murderer.**
2. the **murder weapon.**
3. the **room** in which the murder took place.

When you have finished you must be prepared to justify your decisions to the class!

The Workshop Project

Decrypting the Clues

Clue 1

Clue 1 Answer:

“the room in which the murder was committed has a room number”

HVSFCCAWBKVWQVHVSAIFRSFKOGQE
AAWHHSRVOGOFCCABIAPSF

Caesar Code, Key = 14.

Clue 2

T	R	H	N	R
H	b	A	b	b
E	D	V	H	N
b	O	E	I	A
M	E	b	S	M
U	S	A	b	E
R	b	N	O	b
D	N	b	R	b
E	O	E	b	b
R	T	b	H	b
E	b	I	E	b

Clue 2 Answer:
"the murderer does not have an "e" in his or her name"

TRHNRHbAbbEDVHNbOEIAMEbSM
USAbERbNObDNbRbEOEbbRTbHbE
bIEb

Block Transposition Cipher Key = 5

Clue 3

- Clue 3 Answer:
- “The murder was not in a prime numbered room”
- 20,8,5 13,21,18,4,5,18 23,1,19
  14,15,20 9,14 1 16,18,9,13,5
  14,21,13,2,5,18,5,4 18,15,15,13

- Simple substitution, a=1, b=2, c=3

Clue 4

- Clue 4 Answer:

- “The room number is a multiple of four”

- GSV ILLN MFNYVI RH Z NFOGRKOV LU ULFI
- Caesar code: simple substitution
  A -> Z

Clue 5

- Clue 5 Answer:
- “The murderers name will tell you what country he is from”

- KYV DLIUVIVIJ ERDV NZCC KVCC PFL NYRK TFLEKIP YV ZJ WIFD

- Caesar Shift Cipher, a -> r

Clue 6

Clue 6 Answer:

“the room number has eight factors”

- .... . / .-. --- --- -- / -. ..- -- -... . .-. / .... .- ... / . .. --. .... - / ..-. .- -.-. - --- .-. ... /

Morse code substitution

Clue 7

Clue 7 Answer:

“but how did he do it perhaps with something that students can sit on”

-.- -.. -.-. / --.- -..- ..-. / -- .-. --/ --.- -. / -- -..- / .-. -.-. / -.-- -. .-

--.- .--- -.-- -... / ..-. .-. -.-. --.- / -... -..- ...- -. -.-. --.- .-. .— .--. /

-.-. --.- .--- -.-. / -... -.-. -.. --

-. .-- -.-. -... / .-.. .--- .-- / -...

.-. -.-. / -..- .-- /

Morse code with Caesar shift a → j

The Answer

Who Did it?

Mr Scotland, room 24, chair

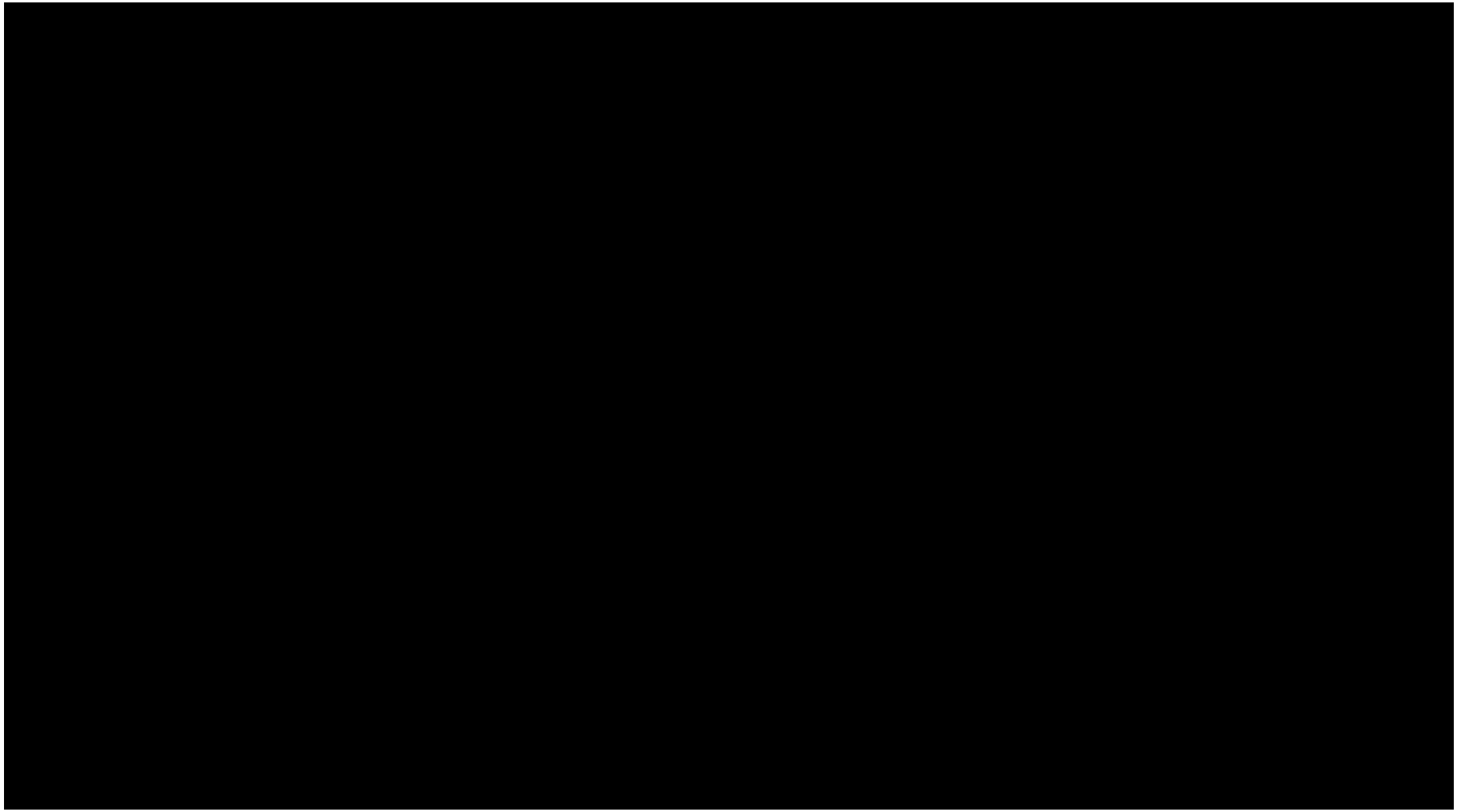
What did we learn today?

- Importance of keeping information secret
- Cryptography – science of enciphering information
- Importance of keys in cipher algorithms
- Use of codes in transmitting information
- Transposition ciphers
- Monoalphabetic substitution ciphers: Caesar and others
- Mixed alphabet ciphers and frequency analysis
- Polyalphabetic ciphers and properties
- Public key cryptosystems – asymmetric keys
- Digital signatures – validating the sender

Careers in STEM

- You must find your passion
- You can have a very rewarding career in science and engineering:
  - Financial, satisfaction, enjoyment
- Need learning and training (education)
- Maybe you will even be another great scientist or engineer!

Careers in STEM



Have Fun Today?

Check out our website:
www.azsciencelab.org
click on the “For Students” tab!

Thanks for coming and exploring with us the world of ciphers!

Long Scytale Message

Fourb**sc**	Line 1
ore**b**and	Line 2
bseven**b**	Line 3
years**b**a	Line 4
go**b**our**b**f	Line 5
orefathe	Line 6
rs**b**broug	Line 7
ht**b**fort	Line 8
h**b**a**b**new	Line 9

Four score and seven years ago our forefathers brought forth…

g o r h h **F** o **b** y o r s t **b** **o** r s e **b** e **b** **b** a **u**

e e a o f b f **b** **r** **b** v r u a r d n **b** a e s r t

o r e **s** n n **b** **b** h u t w **c** d **b** a f e g

The One-Time Pad

1. **Start with the simplest of codes: a=1, b=2, c=3, d=4, etc. Write down message, and corresponding table: For example**

i	l	o	v	e	s	e	c	r	e	t	s
9	12	15	22	5	19	5	3	18	5	20	19

2. **Then arbitrarily "mash" the keyboard with the same number of letters as the message. For example:**

e	d	t	i	l	k	d	f	j	t	p	q
5	4	20	9	12	11	4	6	10	20	16	17

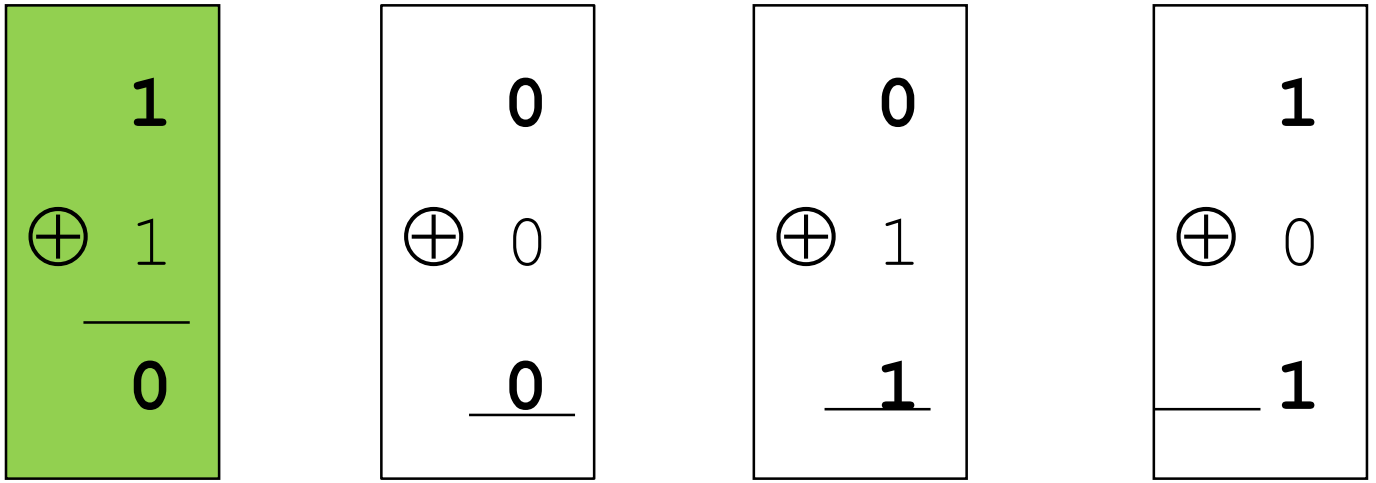
3. **Now add the two strings together. If the number is greater than 26, just wrap it around to the beginning. So, i(9) + e(5) = n(14), and o(15) + t(20) = i(35 - 26 = 9). The result is an encrypted string:**

Decrypting the string to get the secret back is easy. We just subtract the one-time pad: n(14) - e(5) = i(9). Follow that pattern through the entire message.

The one-time pad is totally secure because the bad guys don't know how we got the encoded letter. The n could be i + e, c + k or any other combination.

But there's a flaw. We need to share the one-time pad ahead of time. That could be a problem. If the bad guys get the one-time pad, they would then be able to read everything.

Exclusive OR operation ≡ ⊕



This is a “special” addition with binary numbers

Assume the top row is plaintext and the next row is the key. Then the XOR value is the ciphertext. From this ciphertext you get no information on either the plaintext or key values, because XOR is symmetric.

XOR and encryption

- XOR is used in the public key cryptosystem.
- With long keys – XOR is an unbreakable function.

Riddle: What flower tells what the teacher did after sitting on a tack?

Answer: 10010 01111 10011 00101

Decoded: R O S E

A 00001	H 01000	O 01111	V 10110
B 00010	I 01001	P 10000	W 10111
C 00011	J 01010	Q 10001	X 11000
D 00100	K 01011	R 10010	Y 11001
E 00101	L 01100	S 10011	Z 11010
F 00110	M 01101	T 10100	SPACE 00000
G 00111	N 0110	U 10101	PERIOD 01100

Concealing The Answer

Coded Answer:	10010	01111	10011	00101
Decoded Answer:	R	O	S	E

No Key was used.

So, ROSE is coded using standard ASCII, which everyone knows.

Let's put in a Key, to conceal the answer.

Code ROSE With The Key "JOE"

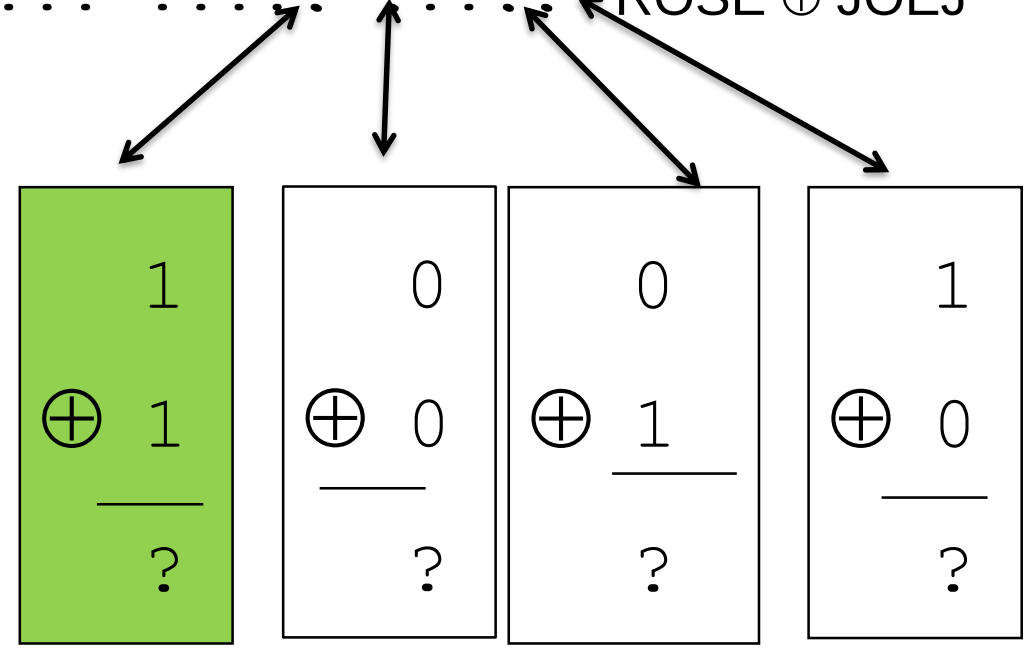
A 00001	H 01000	O 01111	V 10110
B 00010	I 01001	P 10000	W 10111
C 00011	J 01010	Q 10001	X 11000
D 00100	K 01011	R 10010	Y 11001
E 00101	L 01100	S 10011	Z 11010
F 00110	M 01101	T 10100	SP 00000
G 00111	N 01110	U 10101	

```
  10010 01111 10011 00101     ROSE
⊕ 01010 01111 00101 01010     JOEJ (Key= JOE)
-------------------------
  ????? ????? ????? ?????     ROSE ⊕ JOEJ
```

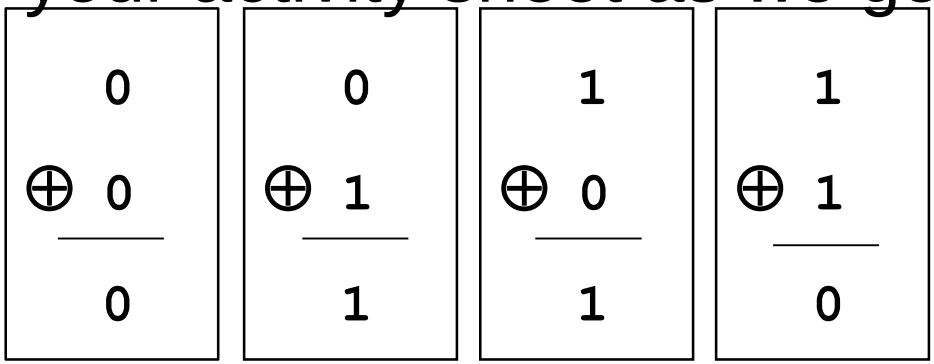
Combine the plaintext and the key by using "⊕"

Coding ROSE With ⊕ JOEJ

```
  10010  01111  10011  00101   ROSE
⊕ 01010  01111  00101  01010   JOEJ (KEY)
 ?????  ?????  ?????  ?????   ROSE ⊕ JOEJ
```



Exercise: ⊕ JOEJ, write the coded and decoded "ROSE" on your activity sheet as we go though them



10010	01111	10011	00101	ROSE
⊕ 01010	01111	00101	01010	JOEJ (Key=JOE)
11000	00000	10110	01111	Coded:ROSE⊕JOEJ
⊕ 01010	01111	00101	01010	JOEJ (Key=JOE)
10010	01111	10011	00101	Decoded:ROSE

ROSE ⊕JOEJ ⊕JOEJ

JOEJ works both ways!

The key is “symmetric under ⊕.”