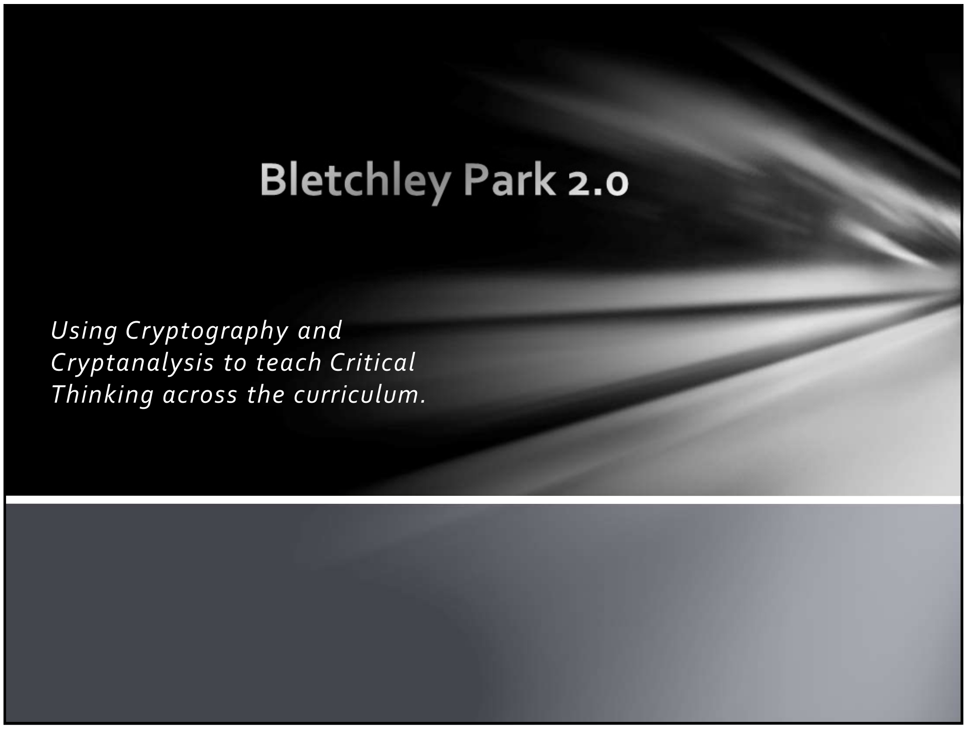
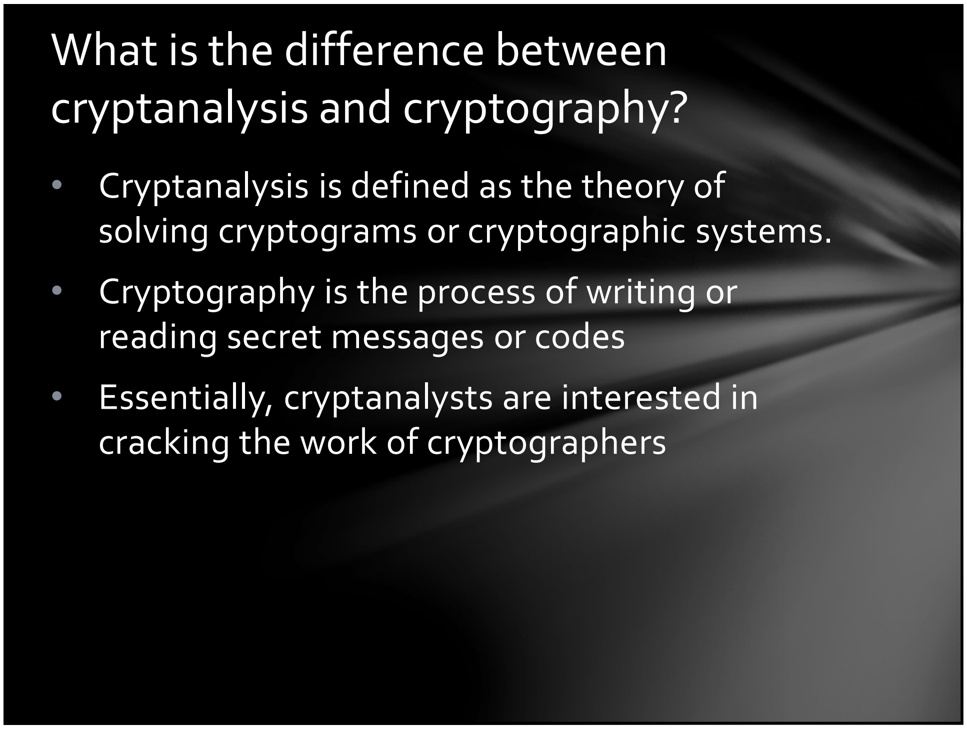


Bletchley Park 2.0

Using Cryptography and Cryptanalysis to teach Critical Thinking across the curriculum.

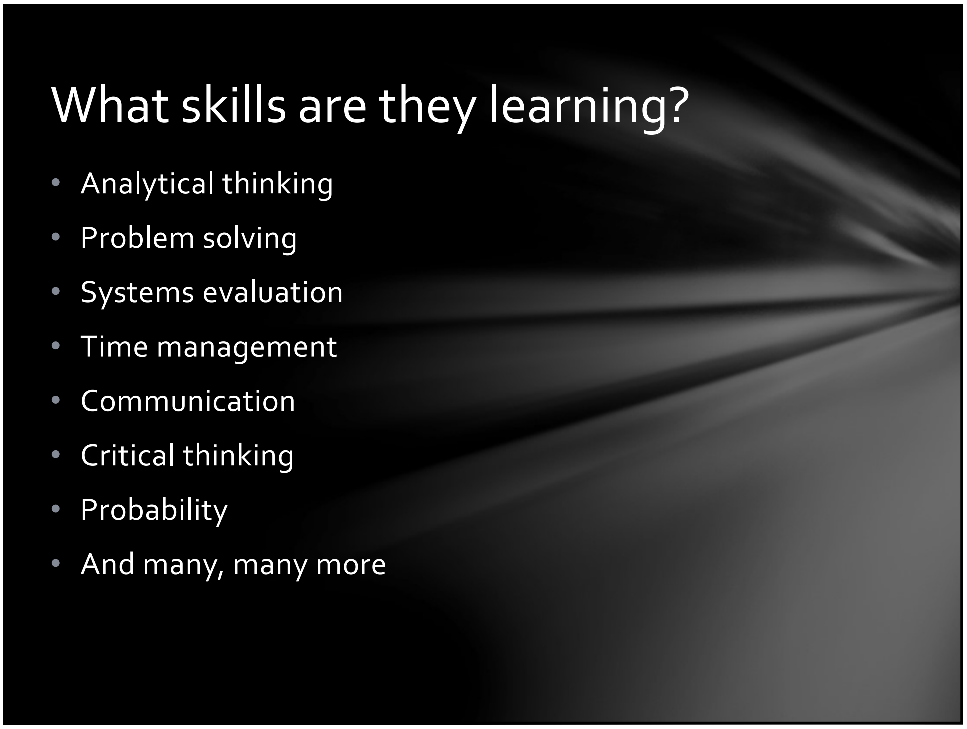
1



What is the difference between cryptanalysis and cryptography?

- Cryptanalysis is defined as the theory of solving cryptograms or cryptographic systems.
- Cryptography is the process of writing or reading secret messages or codes
- Essentially, cryptanalysts are interested in cracking the work of cryptographers

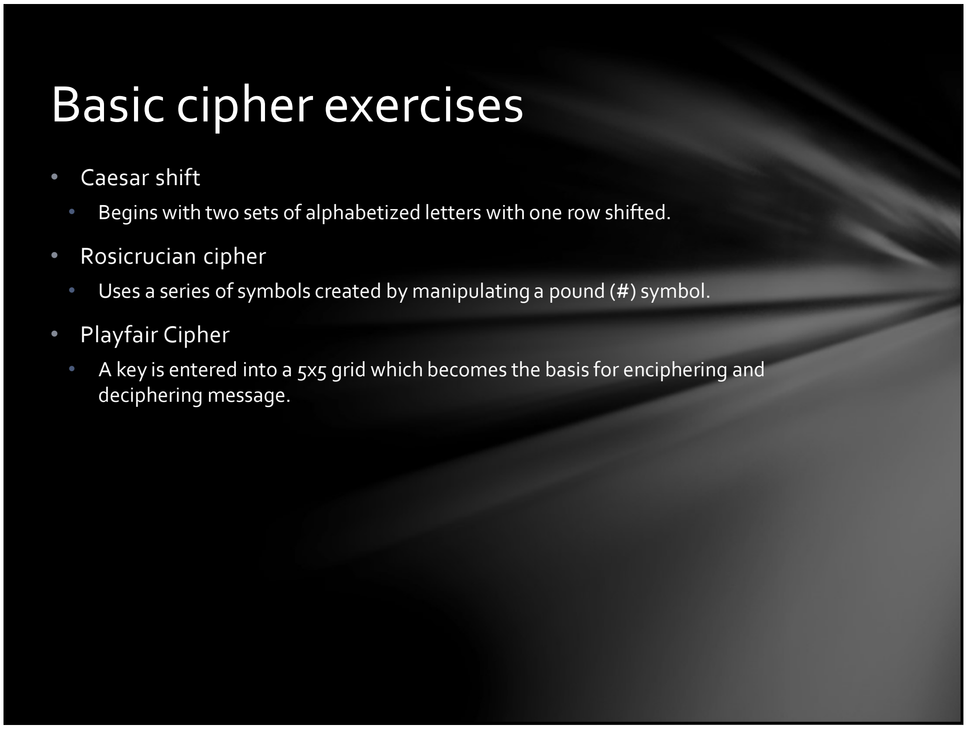
2



What skills are they learning?

- Analytical thinking
- Problem solving
- Systems evaluation
- Time management
- Communication
- Critical thinking
- Probability
- And many, many more

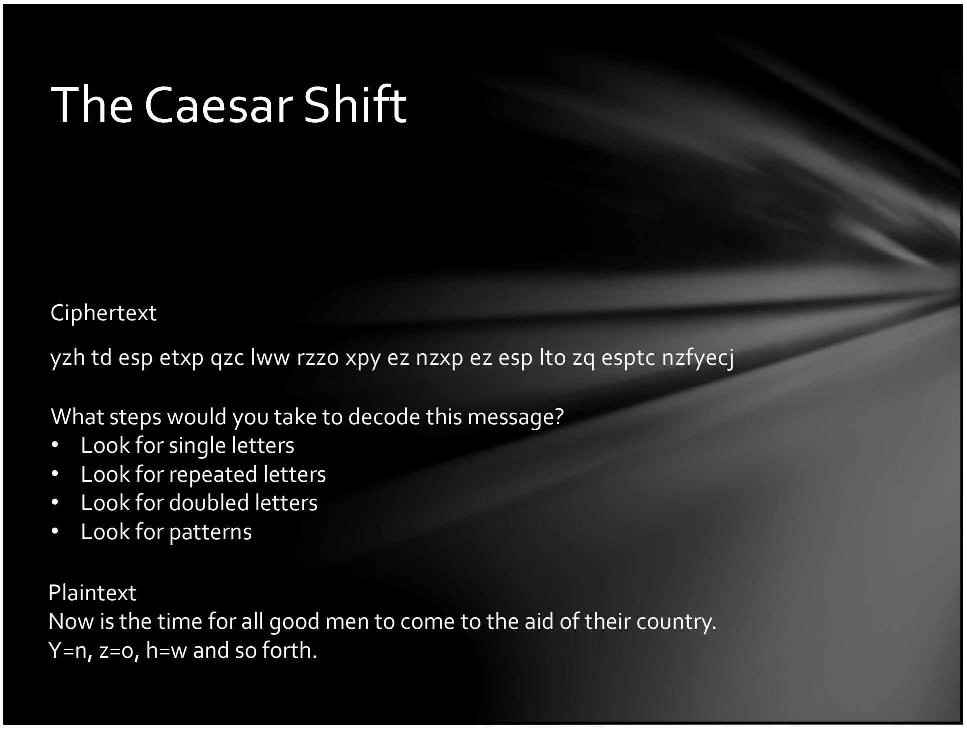
3



Basic cipher exercises

- Caesar shift
  - Begins with two sets of alphabetized letters with one row shifted.
- Rosicrucian cipher
  - Uses a series of symbols created by manipulating a pound (#) symbol.
- Playfair Cipher
  - A key is entered into a 5x5 grid which becomes the basis for enciphering and deciphering message.

4



The Caesar Shift

Ciphertext

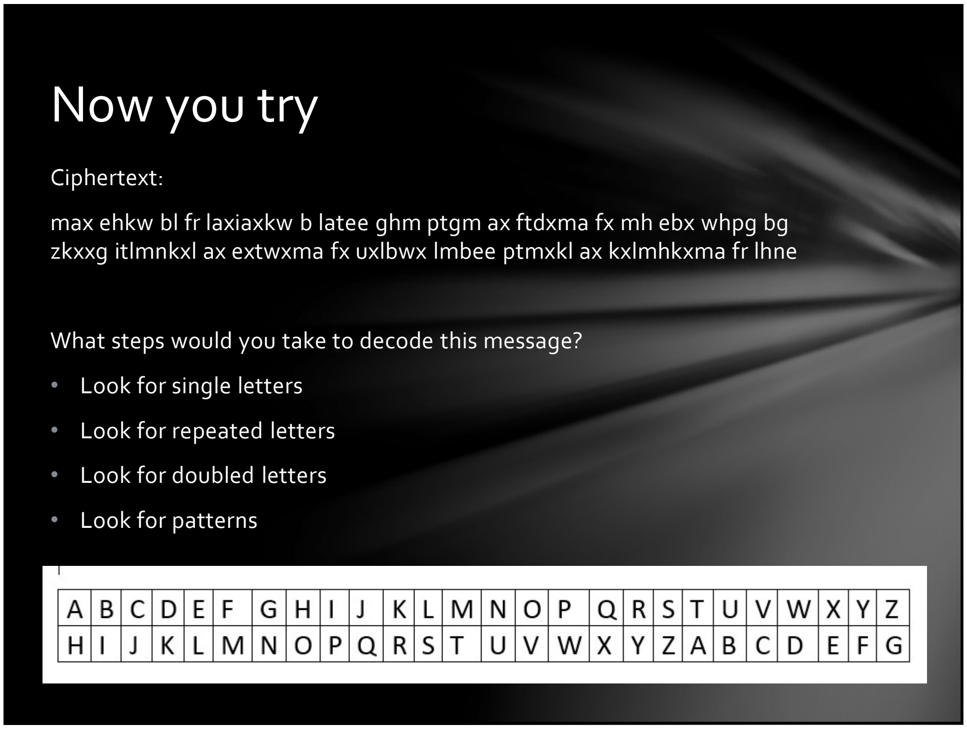
yzh td esp etxp qzc lww rzzo xpy ez nzxp ez esp lto zq esptc nzfyecj

What steps would you take to decode this message?

- Look for single letters
- Look for repeated letters
- Look for doubled letters
- Look for patterns

Plaintext
Now is the time for all good men to come to the aid of their country.
Y=n, z=o, h=w and so forth.

5



Now you try

Ciphertext:

max ehkw bl fr laxiaxkw b latee ghm ptgm ax ftdxma fx mh ebx whpg bg zkxxg itlmnkxl ax extwxma fx uxlbwx lmbee ptmxkl ax kxlmhkxma fr lhne

What steps would you take to decode this message?

- Look for single letters
- Look for repeated letters
- Look for doubled letters
- Look for patterns

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
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

6

The Rosicrucian Cipher

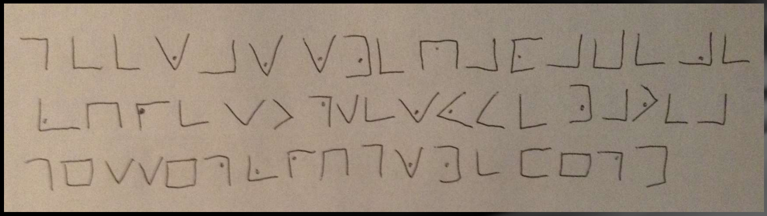
This cipher allegedly goes back centuries to the Rosicrucians. It's a pictogram rather than a lettered cipher and is slightly tougher to crack than a Caesar shift.

- Encoding is based on three sets of pictograms created (usually) from 2 # signs and 2 X's and the use of dots or other symbols within each # and X.
- Can be used in conjuction with other letter based codes for more security.
- If the key is ever compromised, it can be discarded and changed with ease.

7

Example of a Rosicrucian Cipher

Cipher Text

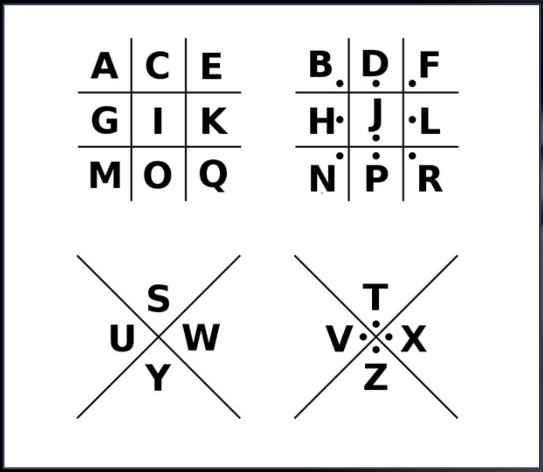


Plain text

Meet at the palace before sunset. We have a mission from the king.

8

Key to the previous code



9

Secret Splitting or Secret Sharing

Secret splitting takes a set of letters or numbers and allows you to break it up so that no one person owns the entire message. This is very difficult to crack because one piece of the cipher is truly random.

Example:

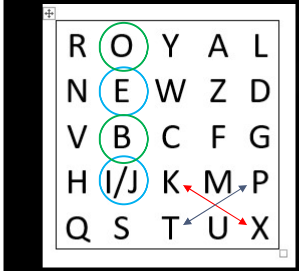
Charlie's Combination:	22 17 39 22
RANDOM KEY:	14 04 07 19
SECOND KEY:	08 13 32 03

This leaves Charlie with the combination, Larry with 1404 0719 and Sammy with 0813 3203. Without the two pieces of the code, Charlie's combination is unknowable.

10

The Playfair Cipher

Playfair was a digram cipher developed by Charles Wheatstone in 1854, but popularized by Lord Playfair and utilized during the Second Boer War and World War I. It was initially rejected by the British War Department for being overly complex.



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

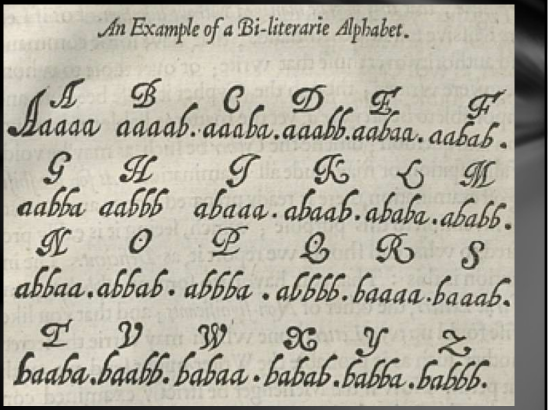
KXJEY UREBE ZWEHE WRYTU HEYFS KREHE GOYFI WTTTU OLKSY CAJPO BOTEI ZONTX BYBWT GONEY CUZWR GDSON SXBOU YWRHE BAAHY USEDQ

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COCE X CREW OF TWELVE X REQUEST ANY INFORMATION X

This typo exists in the original message. Even professionals make mistakes under fire.

11

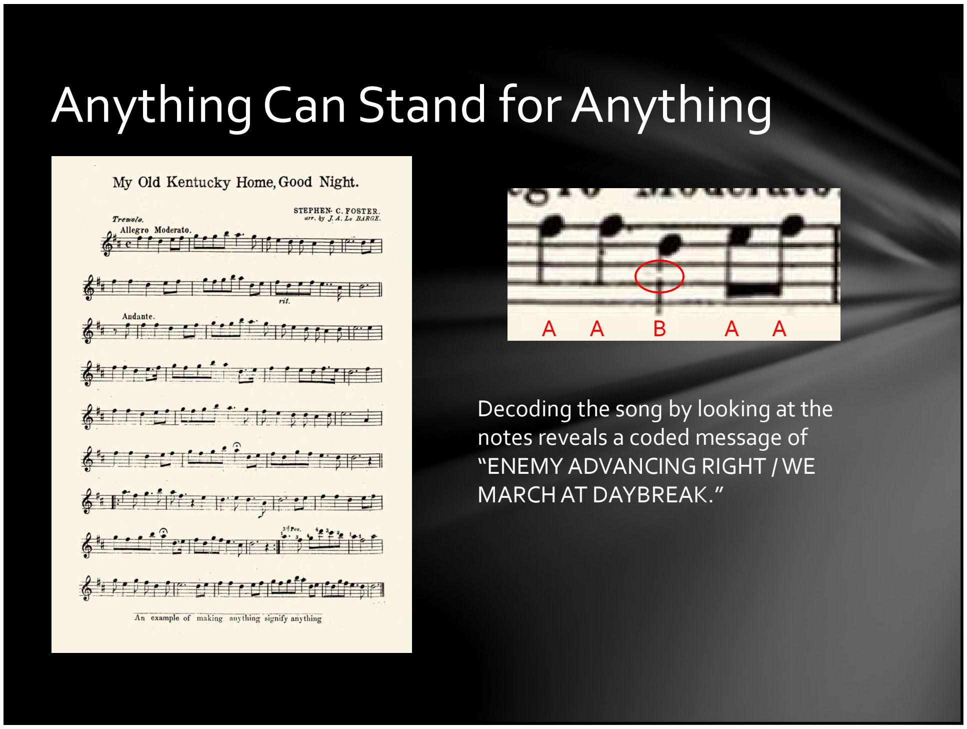
The Friedmans and the Bacon Cipher



An Example of a Bi-literarie Alphabet.

A	B	C	D	E	F
aaaaa	aaaab.	aaaba.	aaabb.	aabaa.	aabab.
G	H	I	K	L	M
aabba	aabbb	abaaa.	abaab.	ababa.	ababb.
N	O	P	Q	R	S
abbaa.	abbab.	abbba.	abbbb.	baaaa.	baaab.
T	V	W	X	Y	Z
baaba.	baabb.	babaa.	babab.	babba.	babbb.

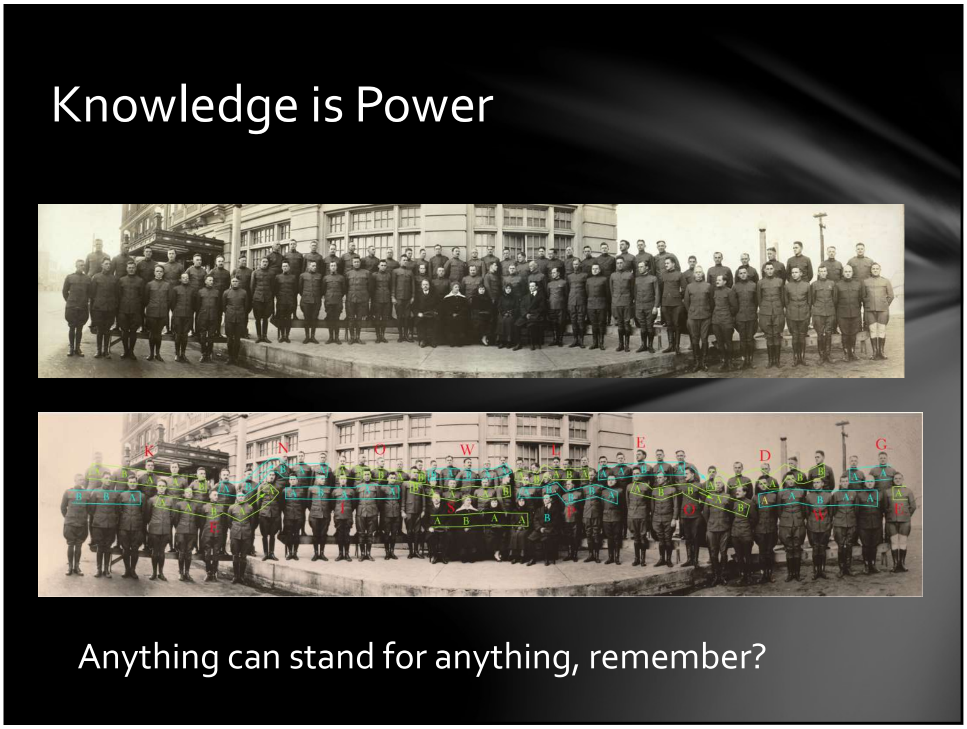
12



Anything Can Stand for Anything

Decoding the song by looking at the notes reveals a coded message of "ENEMY ADVANCING RIGHT / WE MARCH AT DAYBREAK."

13



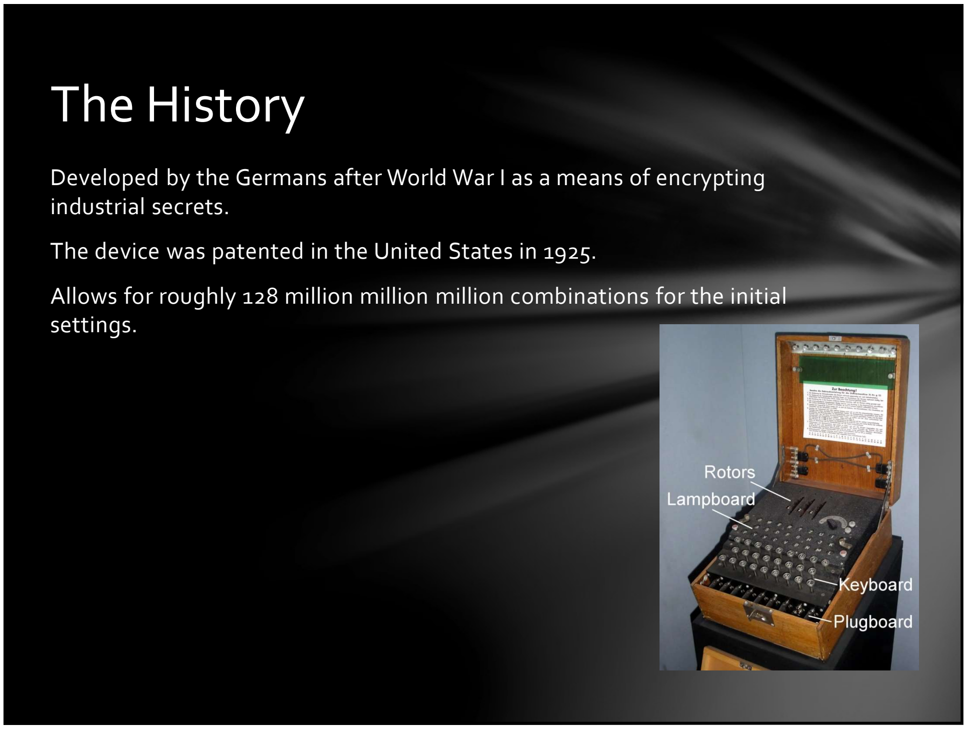
Knowledge is Power

Anything can stand for anything, remember?

14

The ENIGMA Machine

15



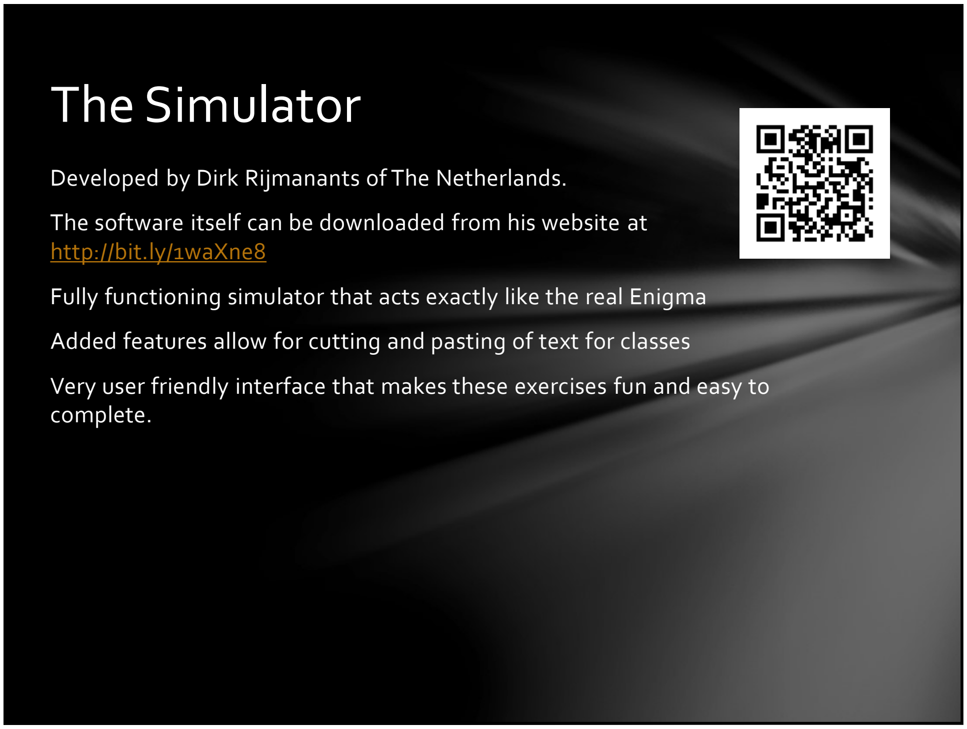
The History

Developed by the Germans after World War I as a means of encrypting industrial secrets.

The device was patented in the United States in 1925.

Allows for roughly 128 million million million combinations for the initial settings.

16



The Simulator

Developed by Dirk Rijmanants of The Netherlands.

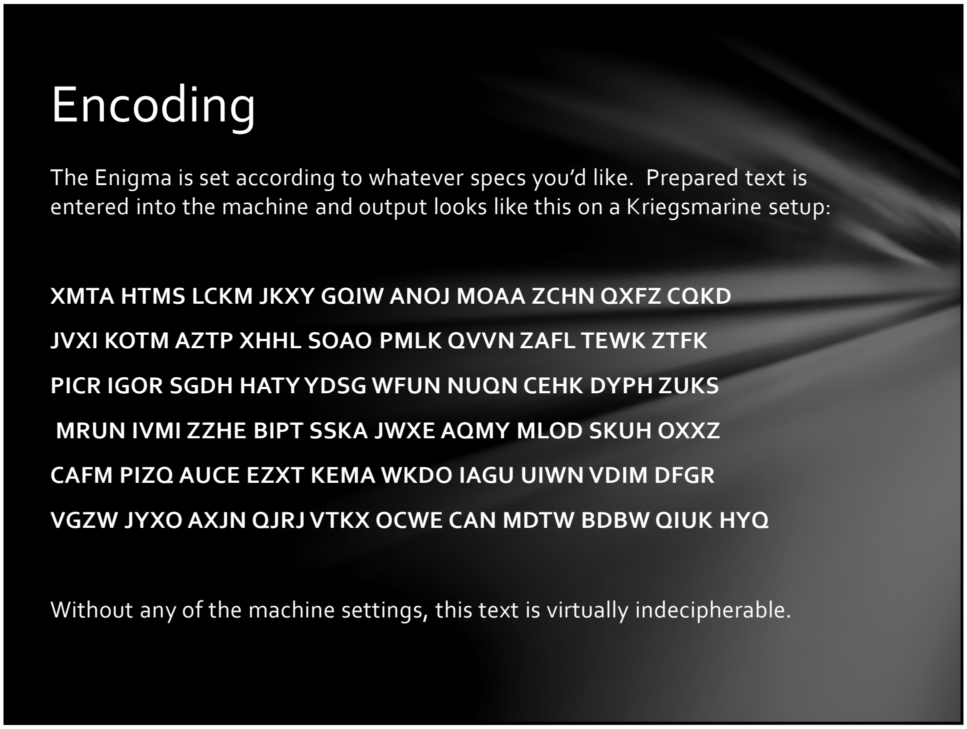
The software itself can be downloaded from his website at http://bit.ly/1waXne8

Fully functioning simulator that acts exactly like the real Enigma

Added features allow for cutting and pasting of text for classes

Very user friendly interface that makes these exercises fun and easy to complete.

17



Encoding

The Enigma is set according to whatever specs you'd like. Prepared text is entered into the machine and output looks like this on a Kriegsmarine setup:

XMTA HTMS LCKM JKXY GQIW ANOJ MOAA ZCHN QXFZ CQKD

JVXI KOTM AZTP XHHL SOAO PMLK QVVN ZAFL TEWK ZTFK

PICR IGOR SGDH HATY YDSG WFUN NUQN CEHK DYPH ZUKS

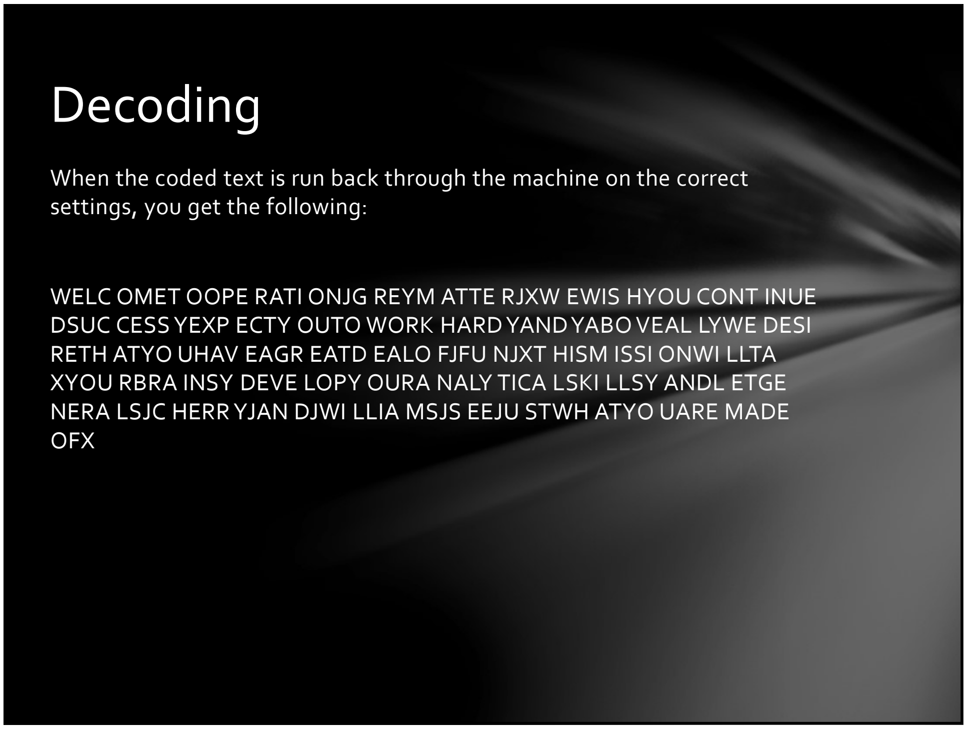
MRUN IVMI ZZHE BIPT SSKA JWXE AQMY MLOD SKUH OXXZ

CAFM PIZQ AUCE EZXT KEMA WKDO IAGU UIWN VDIM DFGR

VGZW JYXO AXJN QJRJ VTKX OCWE CAN MDTW BDBW QIUK HYQ

Without any of the machine settings, this text is virtually indecipherable.

18

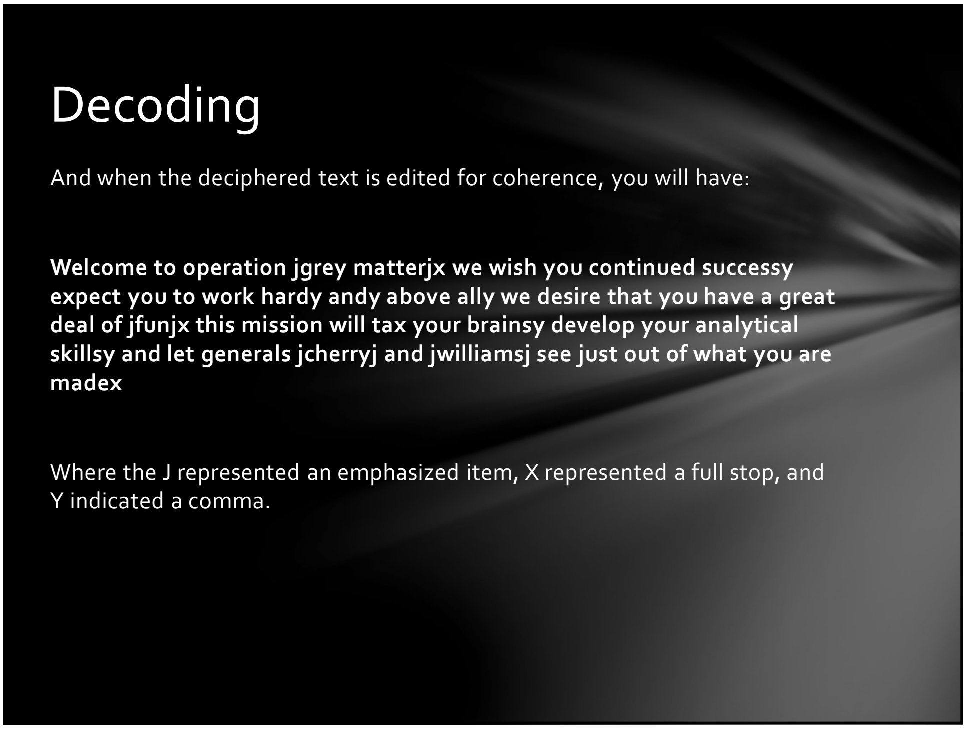


Decoding

When the coded text is run back through the machine on the correct settings, you get the following:

WELC OMET OOPE RATI ONJG REYM ATTE RJXW EWIS HYOU CONT INUE DSUC CESS YEXP ECTY OUTO WORK HARD YAND YABO VEAL LYWE DESI RETH ATYO UHAV EAGR EATD EALO FJFU NJXT HISM ISSI ONWI LLTA XYOU RBRA INSY DEVE LOPY OURA NALY TICA LSKI LLSY ANDL ETGE NERA LSJC HERR YJAN DJWI LLIA MSJS EEJU STWH ATYO UARE MADE OFX

19



Decoding

And when the deciphered text is edited for coherence, you will have:

Welcome to operation jgrey matterjx we wish you continued successy expect you to work hardy andy above ally we desire that you have a great deal of jfunjx this mission will tax your brainsy develop your analytical skillsy and let generals jcherryj and jwilliamsj see just out of what you are madex

Where the J represented an emphasized item, X represented a full stop, and Y indicated a comma.

20

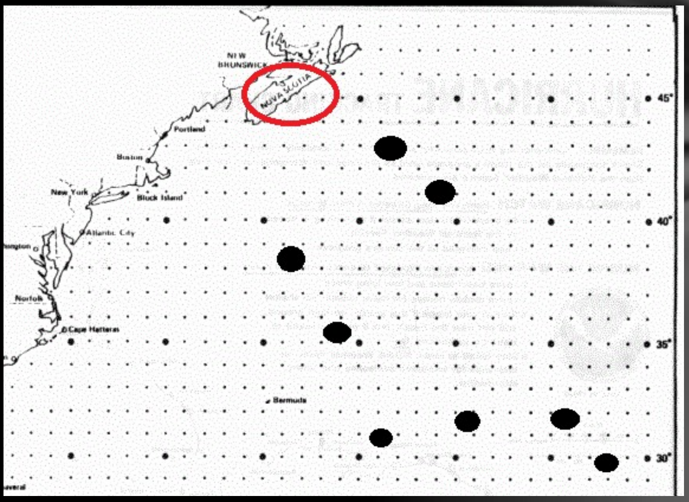
So how do we use it in the classroom?

Our classes were given intercepted code book "remnants" that my co-teacher and I had created with the utility. We then burned them (at home) so that large portions of the necessary information were unavailable, but there was sufficient information to complete the decoding with a little bit of brute force.

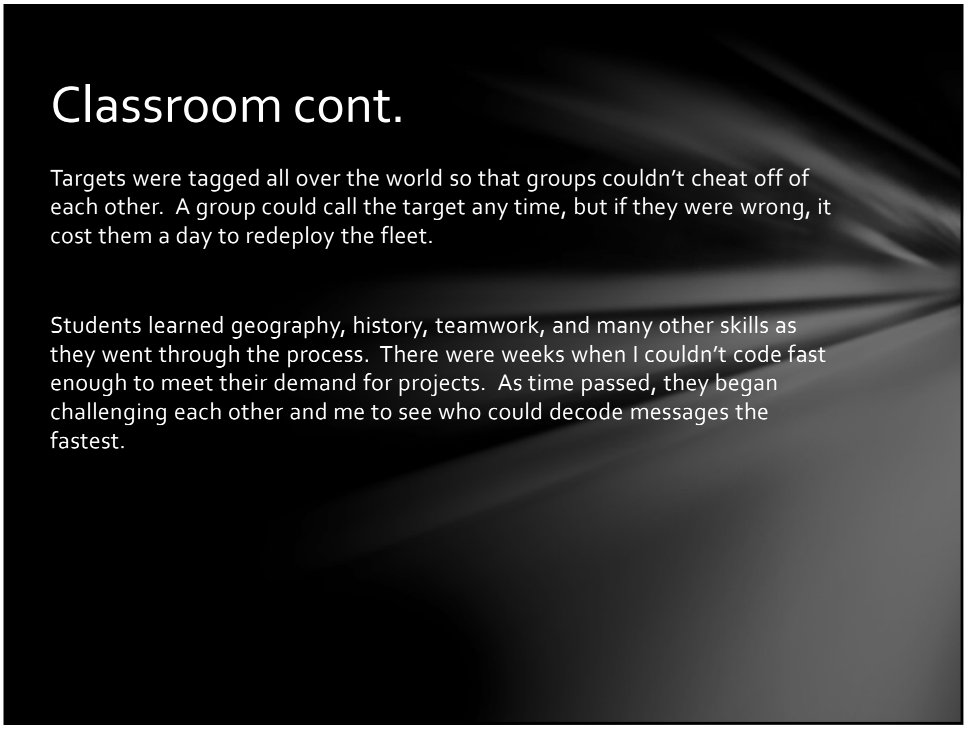
The messages consisted of a series of latitude and longitude coordinates along with orders to travel a certain distance by a certain time. They were to use a hurricane tracking map to plot the location of a U-Boat and determine where the attack was headed. Each hour of class represented one day of travel for the U-Boat. If they decoded all of the messages before time was up, the U-Boat was sunk. If not, the target was destroyed.

21

Sample U-Boat tracking



22

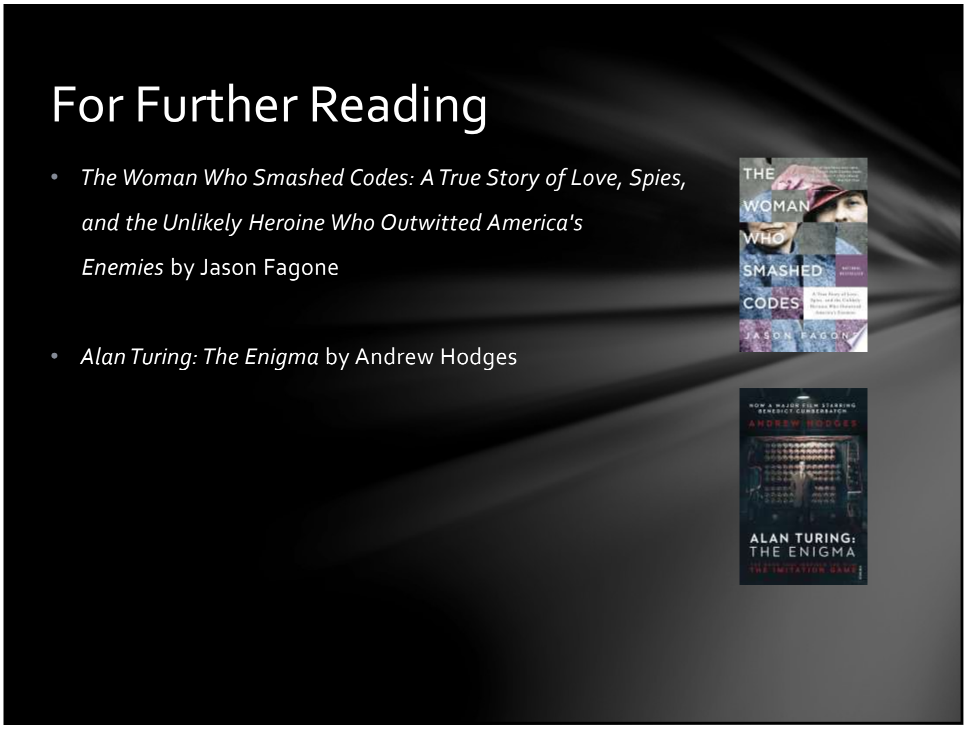


Classroom cont.

Targets were tagged all over the world so that groups couldn't cheat off of each other. A group could call the target any time, but if they were wrong, it cost them a day to redeploy the fleet.

Students learned geography, history, teamwork, and many other skills as they went through the process. There were weeks when I couldn't code fast enough to meet their demand for projects. As time passed, they began challenging each other and me to see who could decode messages the fastest.

23

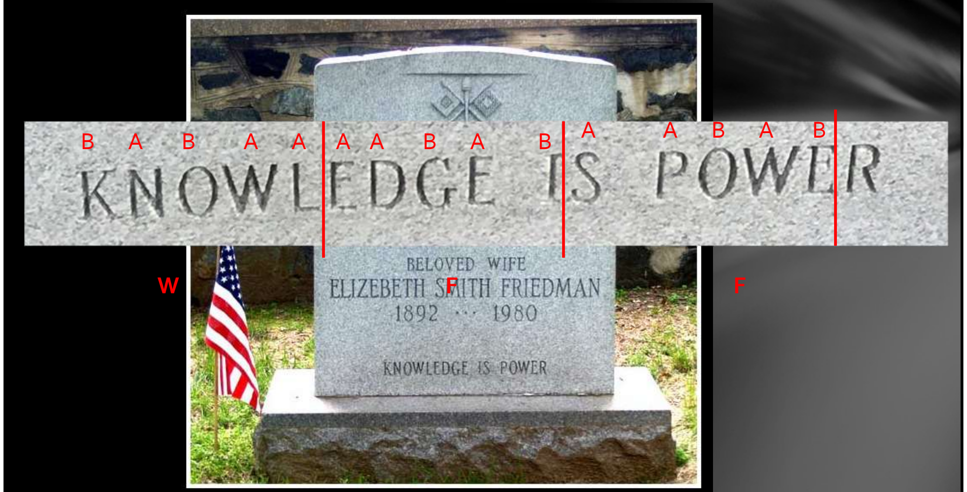


For Further Reading

- *The Woman Who Smashed Codes: A True Story of Love, Spies, and the Unlikely Heroine Who Outwitted America's Enemies* by Jason Fagone
- *Alan Turing: The Enigma* by Andrew Hodges

24

A Fitting Epitaph



25

Links and Contact info

Enigma Machine simulator and codebook generator

http://users.telenet.be/d.rijmenants/index.htm

Wayne Cherry

Librarian/Instructional Technologist

Engineering Instructor

St. Pius X High School

713-579-7571

cherryw@stpiusx.org

@WRCLibrarian

26