Introduction
To Cryptography

Patrick Kellogg

patrickkellogg@gmail.com

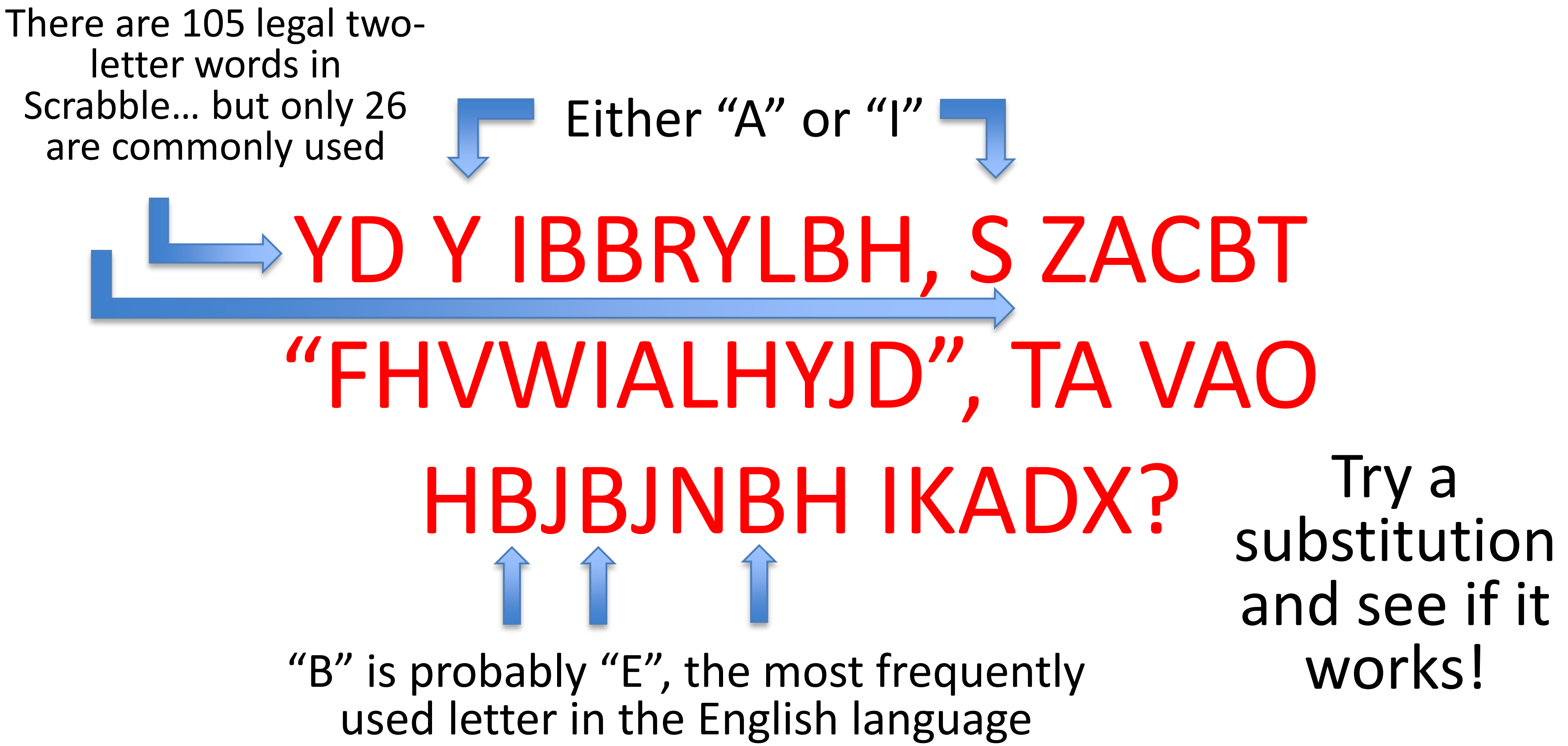
http://www.patrickkellogg.com/kryptos

AS A TEENAGER, I LOVED “CRYPTOGRAMS”, DO YOU REMEMBER THOSE?

YD Y IBBRYLBH, S ZACBT “FHVWIALHYJD”, TA VAO HBJBJNBH IKADX?

How do you solve a cryptogram?

AS A TEENAGER, I LOVED "CRYPTOGRAMS", DO YOU REMEMBER THOSE?



There are 105 legal two-letter words in Scrabble… but only 26 are commonly used

Either "A" or "I"

YD Y IBBRYLBH, S ZACBT "FHVWIALHYJD", TA VAO HBJBJNBH IKADX?

Try a substitution and see if it works!

"B" is probably "E", the most frequently used letter in the English language

- Letter frequency
  - The most common letters in the English language are:

    e t a o i n s r h l d c u m f p g w y b v k x j q z
- Word frequency
  - Try the most frequent two-letter words (or three, or four!)

    of, to, in, it, is, be, as, at, so, we, he, by, or,
    on, do, if, me, my, up, an, go, no, us, am

AS A IEERALBH, S ZACET
“FHVWIALHAJS”, TA VAO
HEJEJNEH IKASX?

Trial and error: do a substitution and see if it works

Historically, military ciphers made it much harder by:

- Removing all spaces between words
- Introducing random letters or “noise”
- Creating a “code” (more about this later)

YDYZIBBRYZLBHSZACZBTFZHVWIA
LHYZZJDTAVAOHBJBJZNBHIKADZX

More ways to solve a cryptogram

- Guess a “crib”
  - A crib is a word that might be in the message. For example, during WWII, British cryptanalysts guessed that many messages started with the phrase KEINEBESONDERENEREIGNISSE: *no special occurrences, nothing to report*. This is a “known-plaintext attack” (KPA)

More ways to solve a cryptogram

- Do a more complex frequency analysis
  - Don’t just look at just the frequency of all letters (etaoin...) but also the frequency of the most common FIRST letters of each word T O A W B C D S F M R H I Y E G L N P U J K) or the frequency of the most common FINAL letters (E S T D N R Y F L O G H A K M P U W)
- Create a custom frequency dictionary based on examples from the “corpus” (body of work) you are studying
  - Count up the letters in any decrypted message you have any use those frequencies instead

Ciphers aren’t Codes!

- Many people use these words interchangeably, but they are actually quite different
- Cryptograms are and example of a “cipher” where each letter is replaced using an algorithm
- To create a code, replace important words or phrases (like “factory” or “stormy weather”) with innocuous words like “banana”. That way, the recurring words can’t be used as a crib (for example “BOMB THE BANANA AT DAWN”)
- Often, codes and ciphers are used together. First, the secret message is coded using word or phrase substitution. Then, a cipher replaces each letter

Pros and Cons of Codes

- Pro: Codes are theoretically uncrackable
  - For example “Buffalo buffalo buffalo buffalo” could mean “bomb the factory at dawn” if that’s what the codebook says. You HAVE to have the codebook to unencrypt the message

- Con: Codes require a book to be distributed that is filled with a lookup chart of all the codewords and what they really mean. This can be difficult, especially since the codebook should be changed regularly for everyone in case the code was cracked

Distribution of Codes and Ciphers

If codes can be uncrackable, why not use them instead of ciphers?

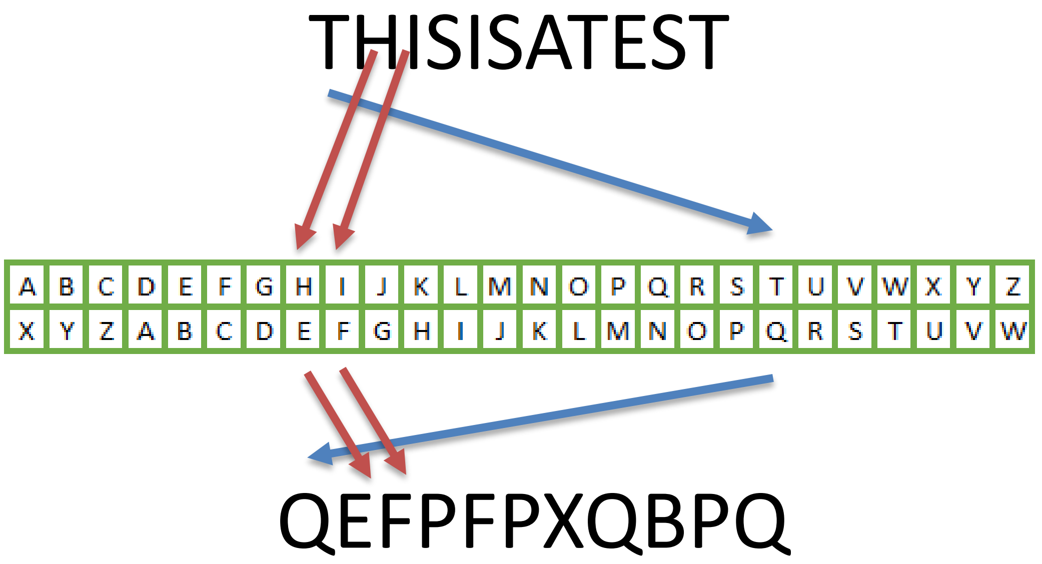
Answer: if even a single codebook is intercepted, security is broken. So, there is often no way to know if your code is secure

To me, this is main driving force for the history of cryptography. How do you keep information out of the hands of the enemy, while making sure that all your friends understand?

The History of Cryptography

The first recorded cipher is the “Caesar cipher” (or “shift cipher”), reportedly used by Julius Caesar to protect military information

To do this cipher, just shift each letter forward or backward in the alphabet



THISISATEST

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
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

QEFPFPXQBPQ

“ROT23” rotating forward 23 letters (i.e. back 3)

More on the Caesar Cipher

- The most famous Caesar Cipher is made by shifting the alphabet forward half-way by 13 letters. Often called “ROT13”, this technique is nice because a second ROT13 will decrypt the message back again

- However, Caesar ciphers are VERY easy to break, since any computer only needs 25 tries to cycle through all shifts of the alphabet. Some people have even taught themselves to read ROT13 messages still encrypted!

One-time Pads

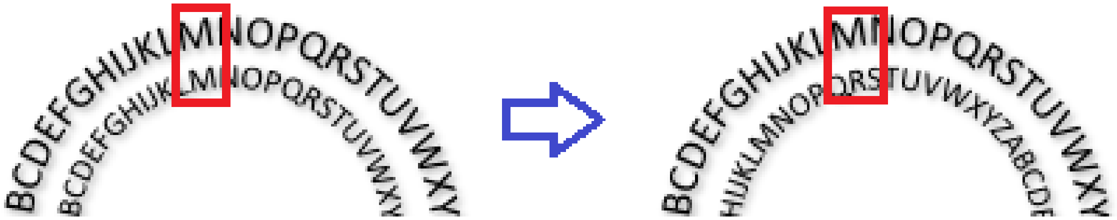
- To make a substitution cipher uncrackable, you can specify the shift of each letter in the message. For example, if given the message is:

  OEHDP… and the shift is [5, 10, 25, 1, 4, …] then you
  shift the first letter (O) ahead 5 places to get (T)
  and shift the second (E) ahead 10 places to get (O)
  to find the start of the message is “TO…”

- For complete security, publish a new “pad” for every message. However, this method will have this same distribution problem as code book did earlier where pads will get stolen and need to be replaced securely

Cipher Disks

- In 1467, an Italian named Leon Battista Alberti came up with idea of creating a little metal disk that would rotate change the letter substitutions



M = M

Replace M with R

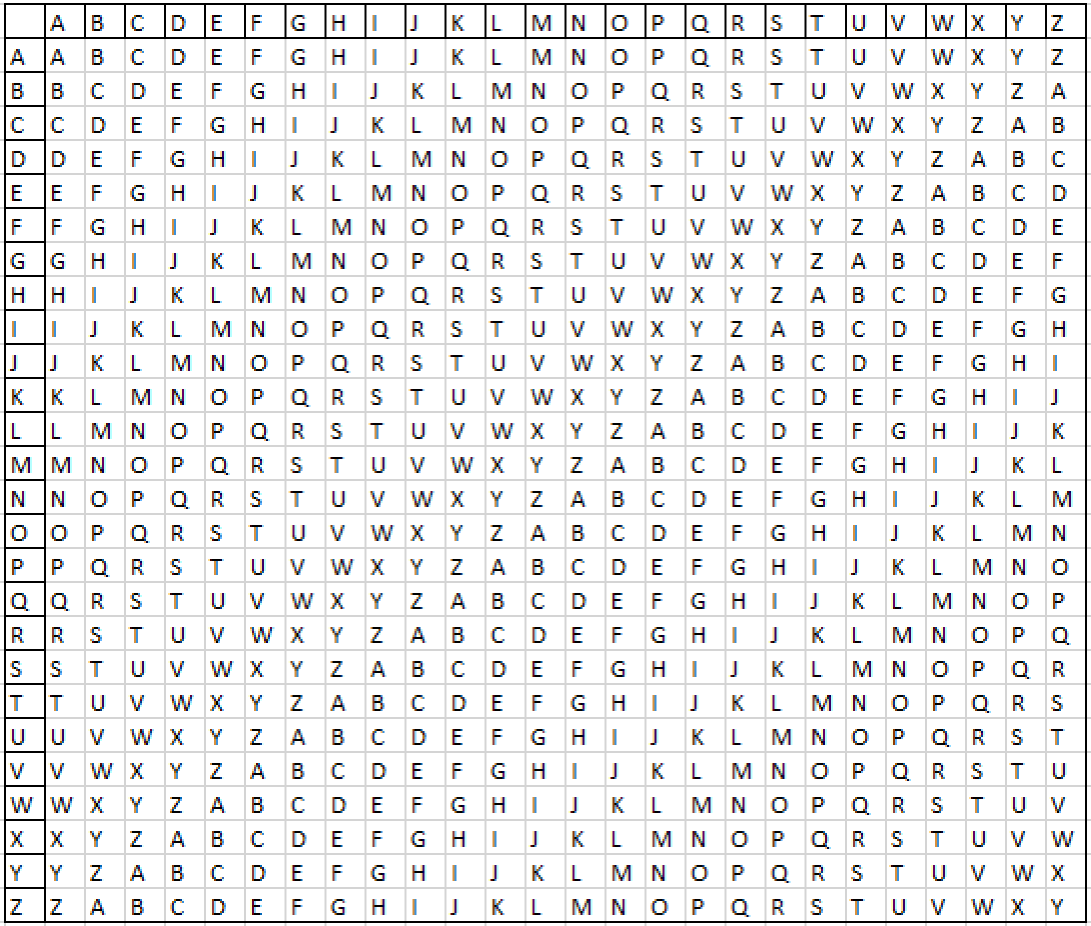
- These were still used during US Civil War by both sides
- In 1934, the chocolate malt drink “Ovaltine” famously gave out a “secret decoder pin” to children who listened to their radio programs

Vigenère Cipher

- Actually not invented by Blaise de Vigenère due to a bad translation. Instead, has its roots in a 1553 book by Giovan Battista Bellaso
- A great compromise between a one-time pad and an easy-to-crack ROT13 is a Vigenère cipher
- To create a Vigenère cipher, come up with a plaintext message you'd like to encrypt, and a keyword

How To Create a Vigenère

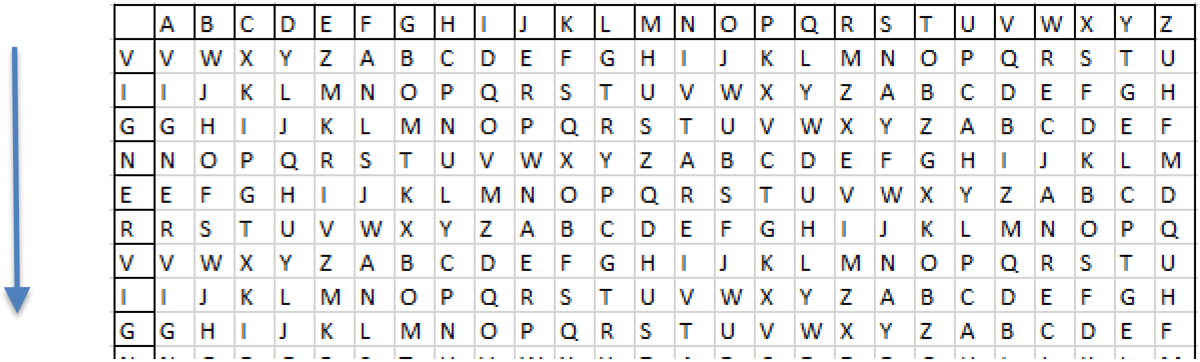
- First write out a table (or “tabula recta”)



	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

How To Create a Vigenère

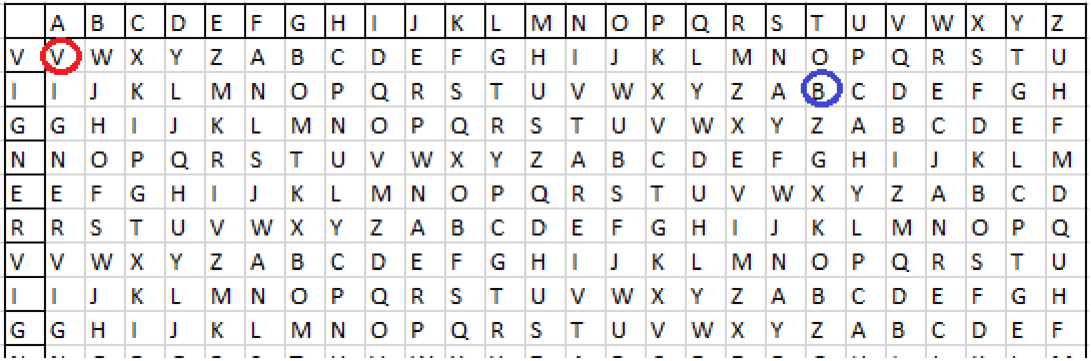
- Take the keyword (for example “Vigenère”) and remove the duplicate “e” letters and repeat it over and over to get “VIGNERVIGNERVIGNERVIGNER”



	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
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
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
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
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
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
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
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
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
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

How To Use a Vigenère

- Take the first letter of the plaintext message to be encoded (like “A” in “ATTACKATDAWN”) and substitute the corresponding keyword letter (“V”)



	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
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
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
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
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
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
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
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
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
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

- For the next letter of the message (“T”), use the lookup on next keyword line (the one starting with “IJKL” line) to get the encrypted letter “B”
- Keep going until the entire plaintext message is encrypted

Vigenère Tips and Tricks

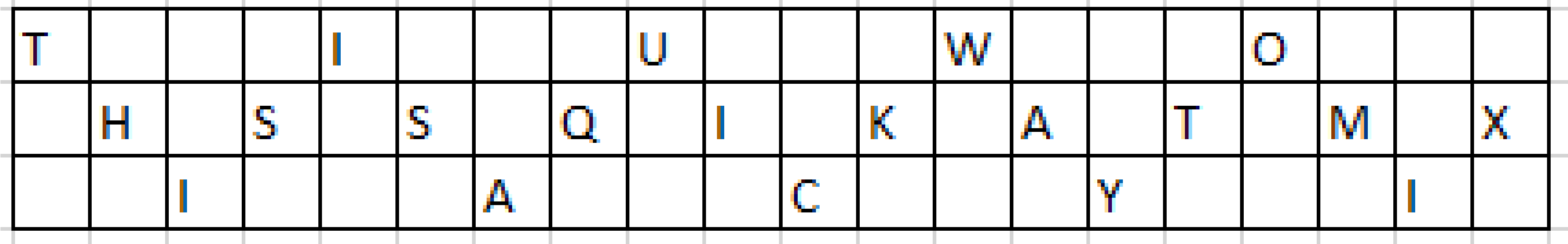
- It helps to have as long a keyword as possible
- Which leads to the problem… if you know the length of the keyword is 6 (“VIGNER”), then you know every sixth letter is going to use the same encryption alphabet, and that helps to decipher it
- The “Enigma engine” that was used (and cracked!) during WWII was a form of substitution cipher using electrical wheels that spun around to create intricate set of encryption alphabets

Transposition Ciphers

- The Caesar and Vigenère ciphers earlier were known as “substitution ciphers” because they replace each letter in the plaintext message with a different letter
- Another method of encrypting a message is to mix up the order of all the letters. This is known as a “transposition cipher”

Rail Fence Cipher

- This is a quick way to mix up the letters in the plaintext message. For example, using the phrase “THISISAQUICKWAYTOMIX”

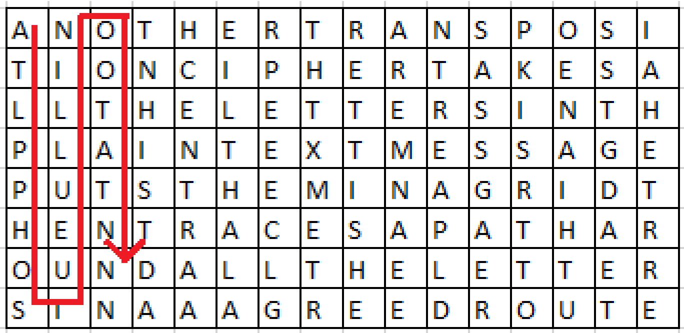


T				I				U				W				O			
	H		S		S		Q		I		K		A		T		M		X
		I				A				C				Y				I	

- Write out the plaintext up and down over 3 rows
- Then, write it out by rows to get TIUWOHSSQIKATMXIACYI

Route Cipher

- Another transposition cipher takes all the letters in the plaintext message, puts them into a grid, and traces a path around all the letters in an agreed route

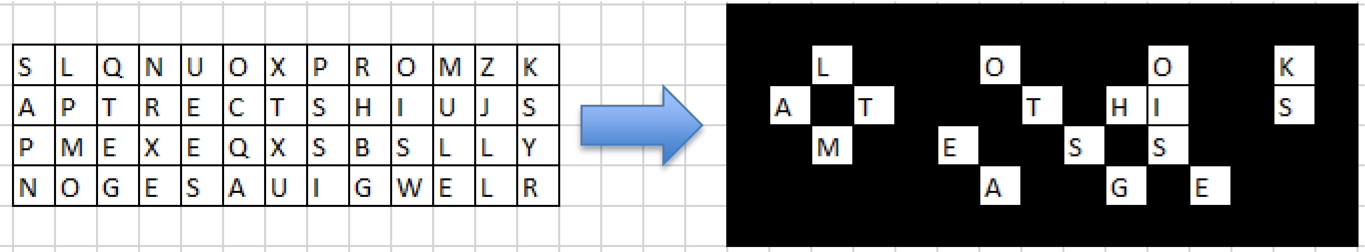


A	N	O	T	H	E	R	T	R	A	N	S	P	O	S	I
T	I	O	N	C	I	P	H	E	R	T	A	K	E	S	A
L	L	T	H	E	L	E	T	T	E	R	S	I	N	T	H
P	L	A	I	N	T	E	X	T	M	E	S	S	A	G	E
P	U	T	S	T	H	E	M	I	N	A	G	R	I	D	T
H	E	N	T	R	A	C	E	S	A	P	A	T	H	A	R
O	U	N	D	A	L	L	T	H	E	L	E	T	T	E	R
S	T	N	A	A	A	G	R	E	E	D	R	O	U	T	E

- This becomes ATLPPHOSIUEULLINOOTATN…
- Or, you could use a different route, like a spiral

Other Transposition Methods

- There are an infinite number of ways to rearrange the letters in a message. For example, there is something called "Myszkowski transposition" that alters the order of the columns. Or, you can use a "grille" which is a piece of paper with holes cut in it.

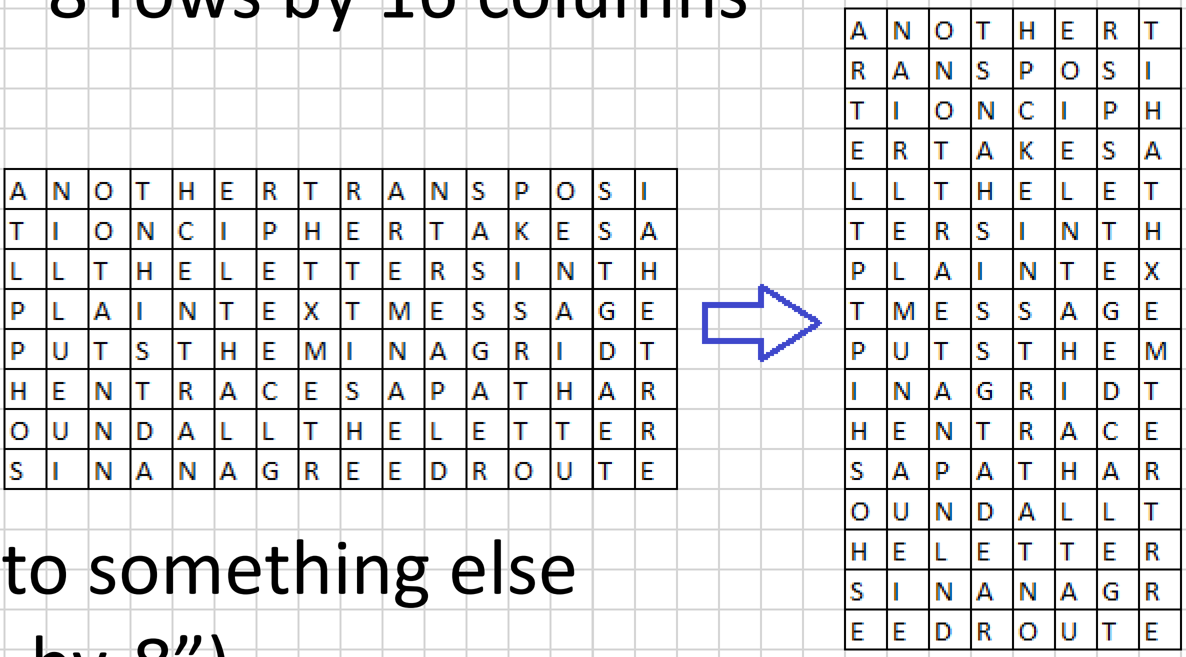


S	L	Q	N	U	O	X	P	R	O	M	Z	K
A	P	T	R	E	C	T	S	H	I	U	J	S
P	M	E	X	E	Q	X	S	B	S	L	L	Y
N	O	G	E	S	A	U	I	G	W	E	L	R

	L				O				O			K
A		T				T		H	I			S
	M			E			S		S			
					A			G		E		

Row-column Transposition

- Take a message with a certain number of columns and rows. For example, our earlier message was "8-by-16" 8 rows by 16 columns



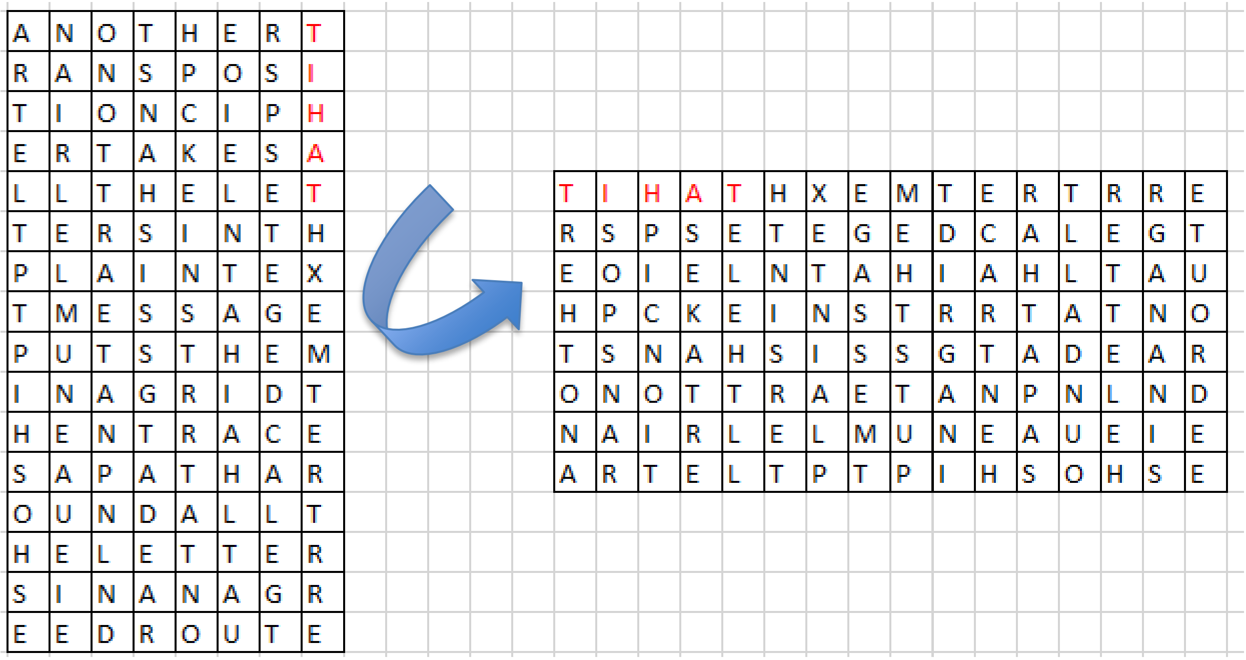
A	N	O	T	H	E	R	T	R	A	N	S	P	O	S	I
T	I	O	N	C	I	P	H	E	R	T	A	K	E	S	A
L	L	T	H	E	L	E	T	T	E	R	S	I	N	T	H
P	L	A	I	N	T	E	X	T	M	E	S	S	A	G	E
P	U	T	S	T	H	E	M	I	N	A	G	R	I	D	T
H	E	N	T	R	A	C	E	S	A	P	A	T	H	A	R
O	U	N	D	A	L	L	T	H	E	L	E	T	T	E	R
S	I	N	A	N	A	G	R	E	E	D	R	O	U	T	E

A	N	O	T	H	E	R	T
R	A	N	S	P	O	S	I
T	I	O	N	C	I	P	H
E	R	T	A	K	E	S	A
L	L	T	H	E	L	E	T
T	E	R	S	I	N	T	H
P	L	A	I	N	T	E	X
T	M	E	S	S	A	G	E
P	U	T	S	T	H	E	M
I	N	A	G	R	I	D	T
H	E	N	T	R	A	C	E
S	A	P	A	T	H	A	R
O	U	N	D	A	L	L	T
H	E	L	E	T	T	E	R
S	I	N	A	N	A	G	R
E	E	D	R	O	U	T	E

- Turn it into something else
  (like "16-by-8")

Double row-column transposition

- Then keep going! As long as the receiver knows the method used to mix up the letters, you could even do a rotation



A	N	O	T	H	E	R	T
R	A	N	S	P	O	S	I
T	I	O	N	C	I	P	H
E	R	T	A	K	E	S	A
L	L	T	H	E	L	E	T
T	E	R	S	I	N	T	H
P	L	A	I	N	T	E	X
T	M	E	S	S	A	G	E
P	U	T	S	T	H	E	M
I	N	A	G	R	I	D	T
H	E	N	T	R	A	C	E
S	A	P	A	T	H	A	R
O	U	N	D	A	L	L	T
H	E	L	E	T	T	E	R
S	I	N	A	N	A	G	R
E	E	D	R	O	U	T	E

T	I	H	A	T	H	X	E	M	T	E	R	T	R	R	E
R	S	P	S	E	T	E	G	E	D	C	A	L	E	G	T
E	O	I	E	L	N	T	A	H	I	A	H	L	T	A	U
H	P	C	K	E	I	N	S	T	R	R	T	A	T	N	O
T	S	N	A	H	S	I	S	S	G	T	A	D	E	A	R
O	N	O	T	T	R	A	E	T	A	N	P	N	L	N	D
N	A	I	R	L	E	L	M	U	N	E	A	U	E	I	E
A	R	T	E	L	T	P	T	P	I	H	S	O	H	S	E

Case Study: Kyptos

- In fact, this method of doing a row-column transposition PLUS a rotation PLUS another row-column transposition AND a Vigenère encryption is all used by an actual unsolved mystery called “Kryptos”
- In the next set of slides, we will look at Kryptos and look into possible methods of solving it!