Ciphers and Thomas Jefferson

Thomas Jefferson and Mathematics Seminar

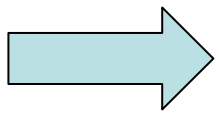
University of Virginia
January 30, 2007

Cipher

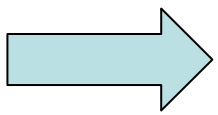
- **Definition:** A *cipher* is a scheme for obscuring a message in order to exchange information securely.
- **Purpose:** To keep a message concealed from all but the intended receiver.
  - Military and government correspondence
  - Secure online transactions (bank account numbers, credit cards)
  - Student information (social security numbers, grades)
  - Personal emails

Terminology

- **Plaintext:** original message, ***P***
- **Ciphertext:** coded message, ***C***
- **Enciphering** or **Encryption:**

P  ***C***

- **Deciphering** or **Decryption:**

C  ***P***

- **Cryptanalysis:** “breaking the code”

Caesar Cipher

- **Replacement** or **Substitution Ciphers**
  - Correspondence between the plain and cipher alphabets
  - Select a number *b,* between 0 and 25, known as the *enciphering shift*
  - Shift the alphabet *b* places
  - Enciphering and deciphering rely on *modular arithmetic*

Caesar Cipher

- Example: *b = 3*

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
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

- Encode the message:
  - *P: THE DUCK FLIES AT NOON*
  - *C: WKH GXFN IOLHV DW QRRQ*

T	H	E	D	U	C	K	F	L	I	E	S	A	T	N	O	O	N
W	**K**	**H**	**G**	**X**	**F**	**N**	**I**	**O**	**L**	**H**	**V**	**D**	**W**	**Q**	**R**	**R**	**Q**

Caesar Cipher, Mathematically Speaking

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example:

P: THE DUCK FLIES AT NOON

Numeric code: **20 8 5 4 21 3 11 1 20 14 15 15 14**

Caesar Cipher, Mathematically Speaking

P: THE DUCK FLIES AT NOON

Numeric code: **20 8 5 4 21 3 11 1 20 14 15 15 14**

- Encipher with *b = 3*
  - Add 3 to each number in the numeric code

23 11 8 7 24 6 14 4 23 17 18 18 17

C: **WKHGXFNIOLHVDWQRRQ**

- How do we decipher this message?

Modular Arithmetic

- Suppose b = 12
  - Plaintext: F L I E S
  - Numeric code: 6 12 9 5 19
  - Numeric ciphercode: 18 24 21 17 (31)
    - Mod 26: 18 24 21 17 5
  - Ciphertext: R X U Q E

Modular Arithmetic

- Decipher

	R	**X**	**U**	**Q**	**E**
– Numeric code:	18	24	21	17	5
– Subtract 12:	6	12	9	5	(-7)
• Or ADD 14:	(32)	(38)	(35)	(31)	19
– Mod 26:	6	12	9	5	19
– Plaintext:	**F**	**L**	**I**	**E**	**S**

Cryptanalysis for the Caesar Cipher

When you do not know the value of *b*

– Brute force method: (25 possibilities)

Numeric ciphercode	*b*	*C* + *b*	Mod 26	"word"
6 12 9 5 19	1	7 12 10 6 20	7 12 10 6 20	GLJFT
6 12 9 5 19	2	8 13 11 7 21	8 13 11 7 21	HMKGU
6 12 9 5 19	3	9 14 12 8 22	9 14 12 8 22	FLIES
6 12 9 5 19	4	10 15 13 9 23	10 15 13 9 23	JOMIW
6 12 9 5 19	5	11 16 14 10 24	11 16 14 10 24	KPNJX

Multiplication Cipher

- Now we designate an enciphering multiplier *a*

  $C = a * P \pmod{26}$

- Only certain values of *a* will work. Can you guess what the criteria is?

Jefferson and Codes

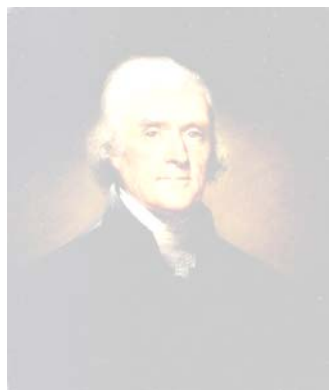
- Jefferson first employed codes when he was the ambassador to France (1784 – 1789)
- Codes were predominantly *nomenclatures*
  - Consisted of 1700 consecutively numbered but randomly arranged words and syllables

Jefferson’s Wheel Cipher

- During his tenure as Secretary of State under George Washington (1790 – 1793), Jefferson devised the wheel cipher to securely encode and decode messages.

The Wheel Cipher: How it looks

- Consisted of 26 cylindrical wooden pieces
- Each cylindrical piece numbered
- Each piece threaded onto an iron spindle
- On the outside of each cylinder the letters of the alphabet were inscribed in random order



Photos from the Monticello web site: www.monticello.org

The Wheel Cipher: How it works

- Stack the disks in a predetermined order
- Spin the disks to display the desired message (plaintext) on one line
- Choose ANY other row as the ciphertext
- Recipient has an identical wheel cipher (wheels in the same order) and spells out the random-seeming letters
- Look for the line that makes sense

Electronic Wheel Cipher

- Designed by three computer science students at UVa:
    - Matthew Spear, Chalermpong Worawannotai, Edward Mitchell

http://www.monticello.org/jefferson/wheelcipher/wheelcipher.html

- “It was very advanced for its time and effectively unbreakable until electronic computers were available.” David Evans, UVa Professor of Computer Science
- Developed independently twice more in history
  - 1890s reinvented by Etienne Bazeries
    - 20 wooden disks
  - M-94 used by the United States from 1923 until 1942
    - 25 aluminum discs

Jefferson's Wheel Cipher

- Very secure if the message is short and the ordering of letters and wheels is not known to the codebreaker
- With 26 disks the number of possible permutations of the disks is:

  $26! > 4*10^{26}$

Drawbacks

- Replicas had to be made and distributed in advance to all of the potential correspondents
- Vulnerable to frequency analysis
- The offset from the plaintext letter to the ciphertext letter for the cipher alphabet on each disk is exactly the same

Lewis and Clark Expedition

- In his official orders to Lewis, issued in April 1803, Jefferson urged Lewis to, “keep him informed at ‘seasonable intervals’ concerning the progress of the expedition, ‘putting into cypher whatever might do injury if betrayed.’
- Wheel cipher not good for an expedition
- No evidence that the cipher was ever used for correspondence

The Vigenère Cipher

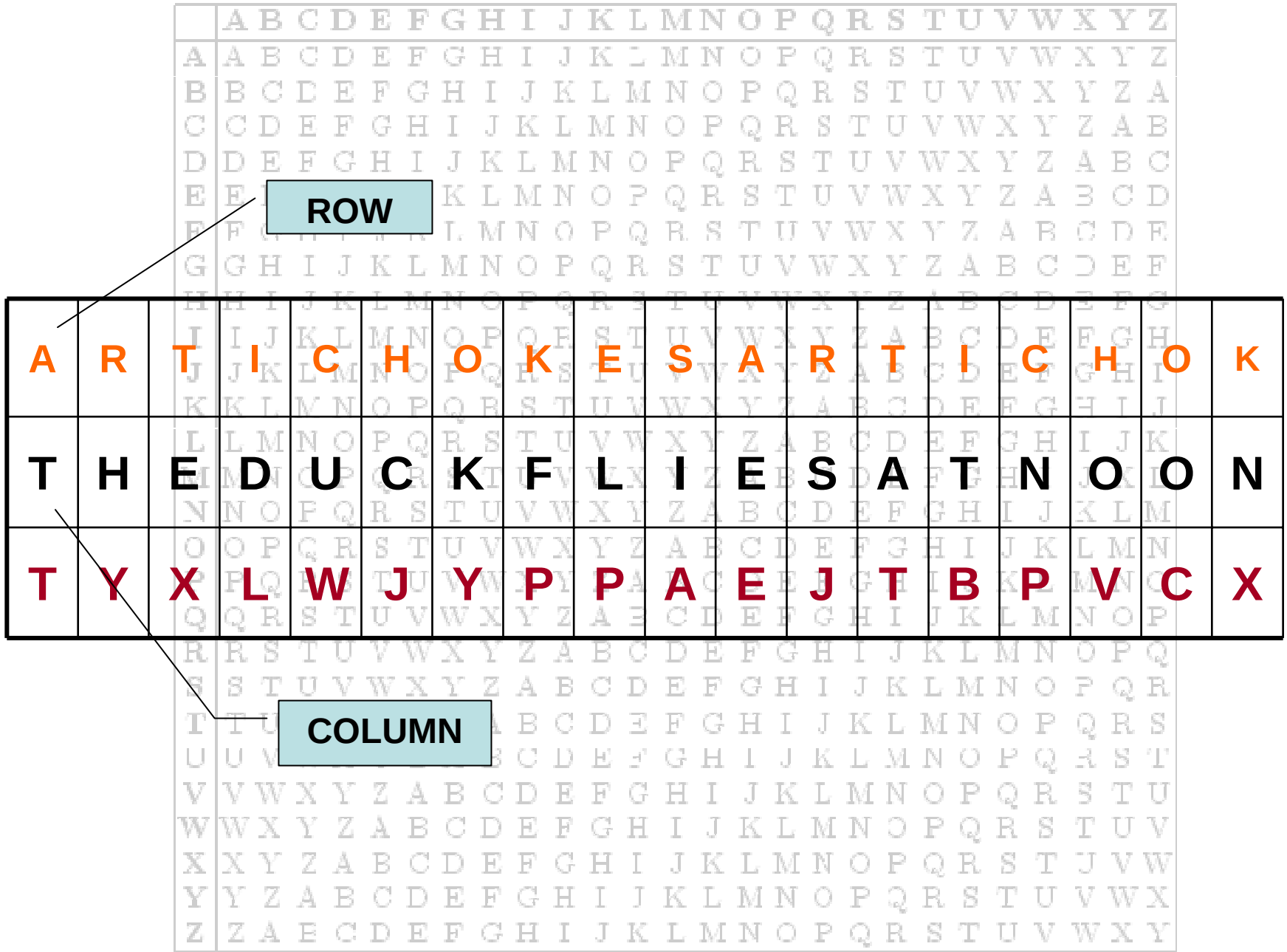
- First proposed by Blaise de Vigenère from the court of Henry III of France in the 16th century
- Thomas Jefferson was assisted by the mathematician Benjamin Patterson in the development of his similar cipher
- Involved only a keyword and memorization of a matrix
- This cipher is a *polyalphabetic substitution*
  - Involves 2 or more cipher alphabets

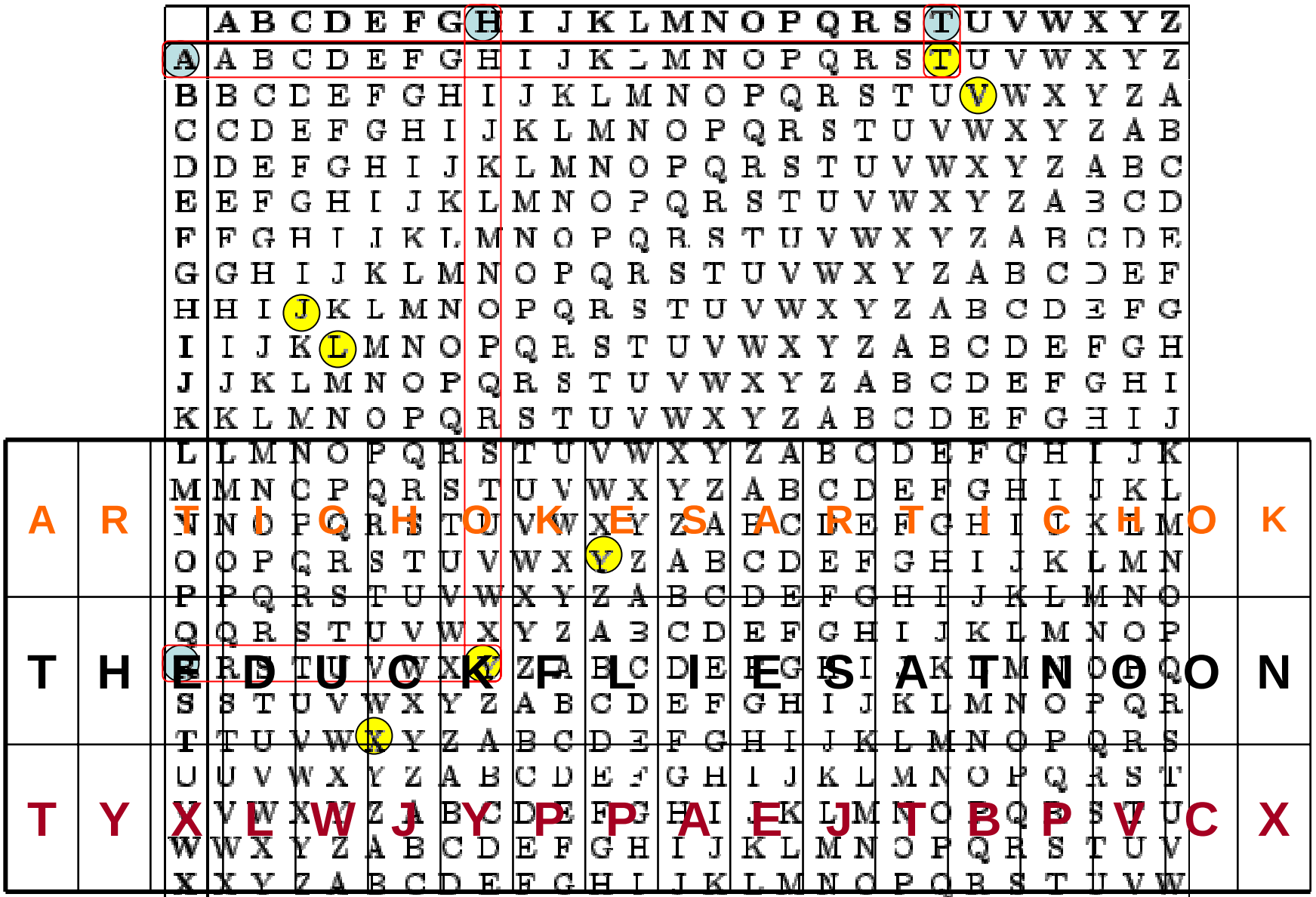
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

The Vigenère Cipher

- Each line is a Caesar cipher
  - The first line corresponds to $b = 0$
  - The last line corresponds to $b = 25$
- To begin, choose a keyword
  - Jefferson and Lewis' keyword: **artichoke**

- Write keyword, repeated as many times as necessary, above the plaintext message
- For each letter in the plaintext, find the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter itself to pick out the ciphertext letter


ROW
A R T I C H O K E S A R T I C H O K
T H E D U C K F L I E S A T N O O N
T Y X L W J Y P P A E J T B P V C X
COLUMN

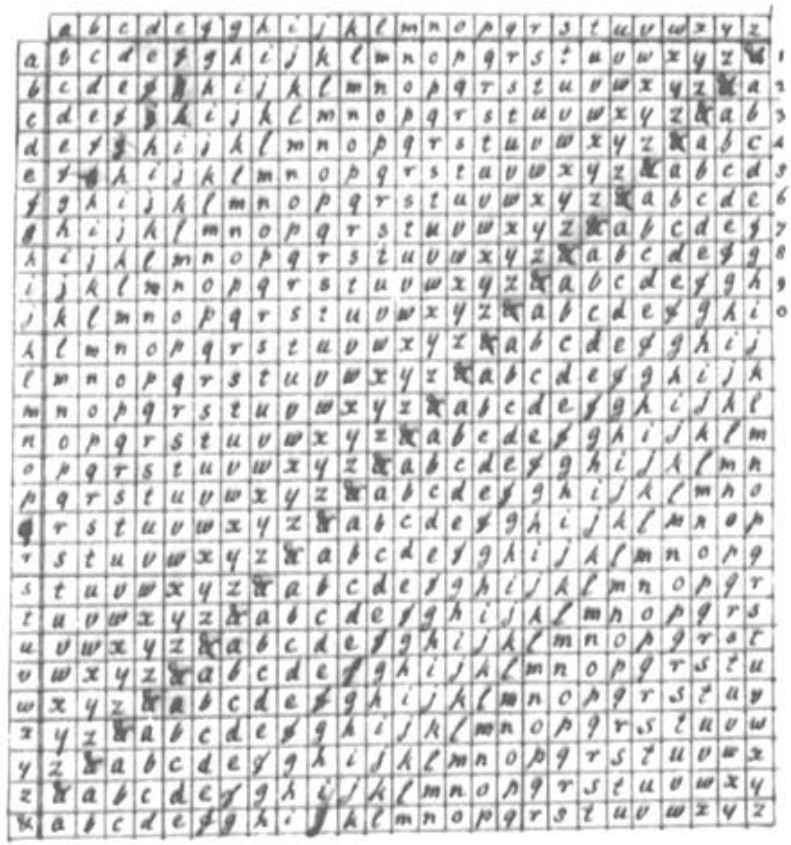

A R T I C H O K E S A R T I C H O K
T H E D U C K F L I E S A T N O O N
T Y X L W J Y P P A E J T B P V C X

The Vigenère Cipher

- Not one-to-one substitution
  - The letter **E** replaced by **X, E**
  - The letter **O** by **V, C**
  - The letter **N** by **P, X**
- More difficult to decipher
- Longer keywords = better encryption
  - A message encrypted is a collection of as many simple substitution ciphers as there are letters in the keyword
- To crack the code, look for patterns of letters to find the length of the keyword (broken in 1863)

The Vigenère Cipher

- Try to decipher the word **SLGLKHZ** with the keyword ***artichoke***
  - Answer: **SUNDIAL**
- Encrypt **THIS IS IT**
  - Keyword ***artichoke*:** **TYBAKZWD**
    - **I** replaced by **B, K, W**
  - Keyword ***of*:** **HMWXWXWY**
    - **I** replaced by **W, W, W**



Suppose the keyword to be 'antipodes'

write it thus a n t i p o d e s a n t i p o d e s a n t i p o d e s
to be cyphered t h e m a n w h o s e m i n d o n v i r t u e b e n t
u v y u g b & m g t s f r c s s s n j e m c u g i t m

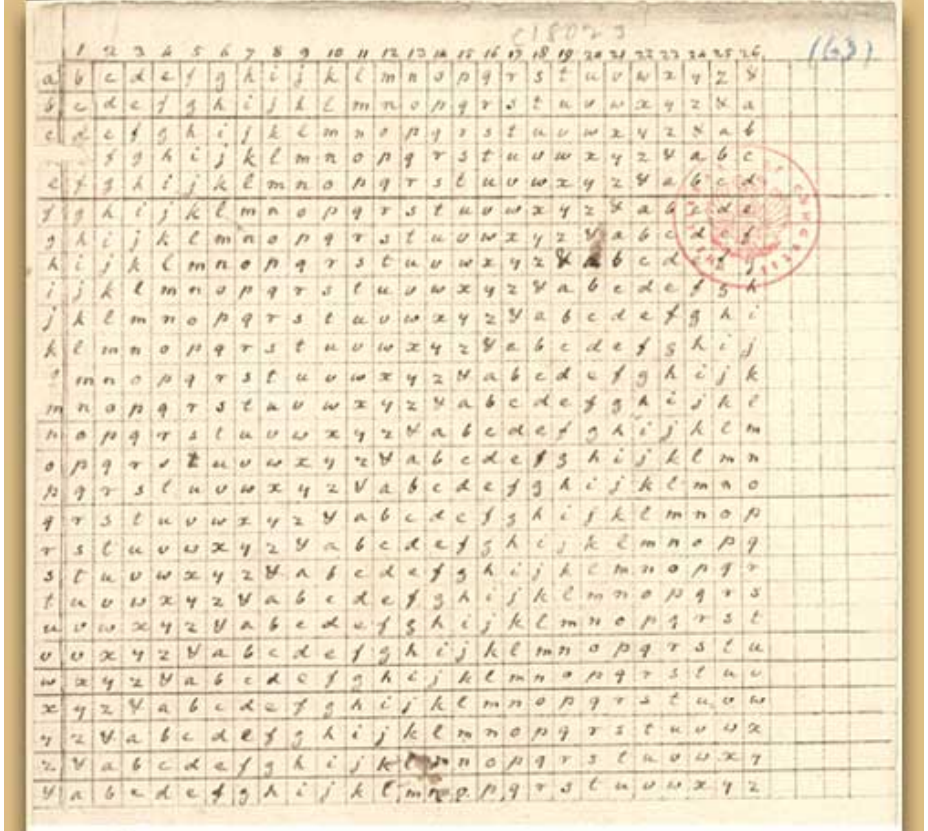
then copy out the cyphered line thus. uvyugb&mgtsfrcsssnjemcugitm

numbers are thus. 18. is *bv.* 1798 is thus *bubq*

the method is this

look for t in the 1st vertical column, & a in the 1st horizontal one, gives u

h . . . . . n v
e . . . . . t . . . . . y
m . . . . . i . . . . . u
a . . . . . p . . . . . q
n . . . . . o . . . . . b



The man whose mind on virtue bent

the equivalent of the 1st line is taken from the 1st col.
of the 2d from the 2d
of the 3d from the 3d.

and so on to the 26th and then begin again with the 1st 2d etc.

or instead of using them in the regular numerical order have a key word suppose 'artichoke' and finding the letter to be cyphered [?] in the 1st column, seek it's equivalent in the column over a

in the last horizontal line & so on as follows

t in the 1st vertical over a in the last horizontal, which is u

h . . . . . t . . . . . z
e . . . . . t . . . . . y
m . . . . . c v
a . . . . . c . . . . . d
n . . . . . h . . . . . u

[See below]