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

C

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

 $P \longrightarrow$

С

- Deciphering or Decryption:
- 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

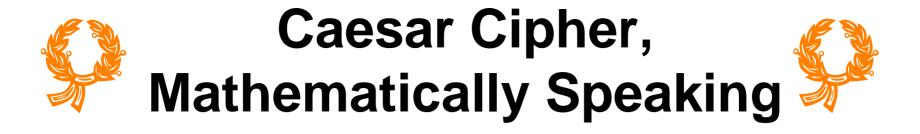


• Example: b = 3

Α	В	С	D	Е	F	G	Н	I	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Ζ
D	Ε	F	G	Н		J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W		Y	Ζ	A	В	С

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

т	Н	Ε	D	U	С	к	F	L	I	Е	S	Α	т	Ν	0	0	N
W	Κ	Н	G	X	F	Ν	I	0	L	Η	V	D	W	Q	R	R	Q



Α	В	С	D	Е	F	G	Η	I	J	К	L	М
1	2	3	4	5	6	7	8	9	10	11	12	13
N	0	Ρ	Q	R	S	Т	U	V	W	Х	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: FLIES
 - Numeric code: 6 12 9 5 19
 - -Numeric ciphercode: 18 24 21 17 (31)
 - Mod 26: 18 24 21 17 5
 - Ciphertext:

RXUQE



Modular Arithmetic



- Decipher
 - Numeric code:
 - Subtract 12:
 - Or ADD 14:
 - -Mod 26:
 - Plaintext:

 R
 X
 U
 Q
 E

 18
 24
 21
 17
 5

 6
 12
 9
 5
 (-7)

 (32)
 (38)
 (35)
 (31)
 19

 6
 12
 9
 5
 19

 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

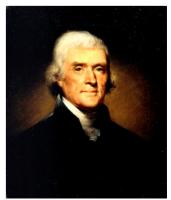
Now we designate an enciphering multiplier a

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

 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/wheelcip her/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

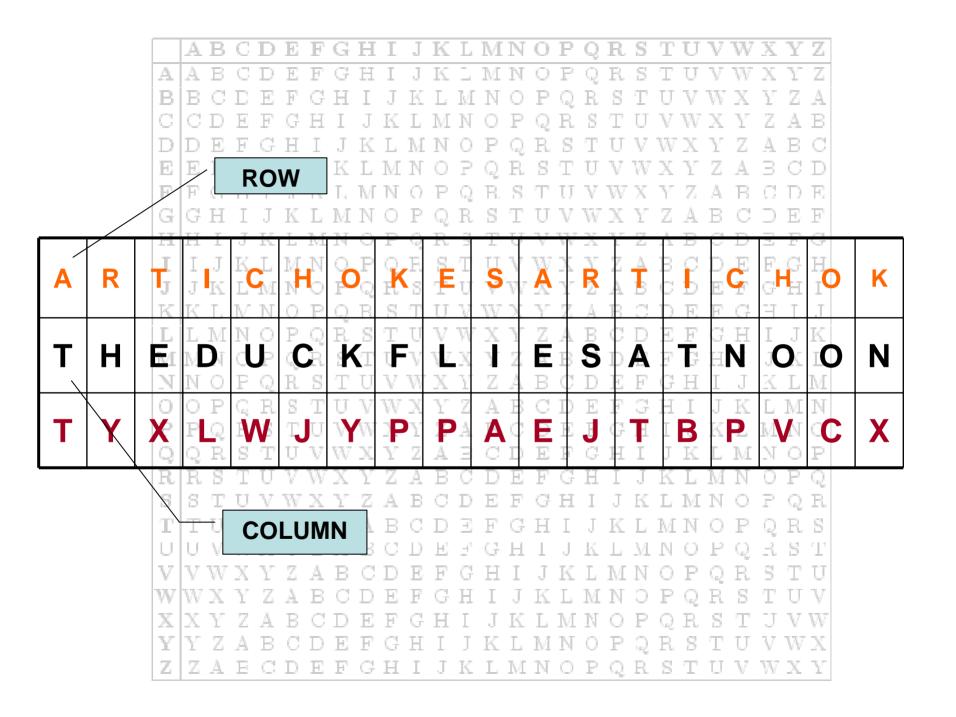
- First proposed by Blaise de Vigenère from the court of Henry III of France in the 16th century
- Thomas Jefferson was assisted by the mathematician Benjamin Patterson in the development of his similar cipher
- Involved only a keyword and memorization of a matrix
- This cipher is a *polyalphabetic substitution*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

	A	В	С	D	Е	F	G	H	Ι	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{Z}
Α	A	В	С	D	Ε	F	G	Η	Ι	J	\mathbf{K}	2	\mathbf{M}	Ν	0	P	Q	R	S	Т	υ	V	W	Х	Y	Ζ
B	B	С	С	\mathbf{E}	F	G	\mathbf{H}	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	\mathbf{Z}	A
С	C	D	Е	\mathbf{F}	G	Η	Ι	J	\mathbf{K}	\mathbf{L}	Μ	Ν	0	Ρ	Q	\mathbf{R}	\mathbf{S}	Т	U	V	W	х	\mathbf{Y}	Ζ	А	В
D	D	Ε	F	\mathbf{G}	Η	Ι	\mathbf{I}	\mathbf{K}	L	\mathbf{M}	Ν	0	Ρ	Q	\mathbf{R}	\mathbf{S}	Т	U	\mathbf{V}	W	х	\mathbf{Y}	\mathbf{Z}	\mathbf{A}	В	\mathbf{C}
\mathbf{E}	\mathbf{E}	\mathbf{F}	G	Η	Γ	J	\mathbf{K}	L	М	Ν	0	Ρ	Q	\mathbf{R}	\mathbf{S}	Т	U	V	W	х	\mathbf{Y}	\mathbf{Z}	А	З	\mathbf{C}	D
F	F	Ģ	Ħ	Т	I.	Κ	Τ.,	М	Ν	0	Ρ	Q	R.	\mathbf{S}	Т	U	V	W	Х	\mathbf{Y}	\mathbf{Z}	A	В	\mathbf{C}	D	E,
G	\mathbf{G}	\mathbf{H}	Ι	J	\mathbf{K}	L	Μ	Ν	0	\mathbf{P}	Q	R	\mathbf{S}	\mathbf{T}	U	V	W	х	\boldsymbol{Y}	\mathbf{Z}	A	В	\mathbf{C}	\supset	Ε	\mathbf{F}
\mathbf{H}	\mathbf{H}	Ι	\mathbf{I}	\mathbf{K}	L	\mathbf{M}	\mathbf{N}	Ο	\mathbf{P}	Q	R	5	\mathbf{T}	U	v	W	х	\mathbf{Y}	\mathbf{Z}	Α	В	\mathbf{C}	D	Ξ	\mathbf{F}	G
Ι	Ι	\mathbf{J}	\mathbf{K}	L	\mathbf{M}	Ν	0	\mathbf{P}	Q	E.	\mathbf{S}	Τ	U	V	W	х	Y	Ζ	А	В	\mathbf{C}	D	Ε	\mathbf{F}	\mathbf{G}	\mathbf{H}
J	J	\mathbf{K}	L	\mathbf{M}	\mathbf{N}	0	\mathbf{P}	Q	\mathbf{R}	\mathbf{S}	Т	U	V	W	х	\mathbf{Y}	\mathbf{Z}	А	В	\mathbf{C}	\mathbb{D}	\mathbf{E}	\mathbf{F}	\mathbf{G}	Η	Ι
Κ	\mathbf{K}	L	\mathbb{M}	\mathbf{N}	0	\mathbf{P}	Q	\mathbf{R}	\mathbf{S}	Т	U	V	W	х	\mathbf{Y}	\mathbf{Z}	А	В	С	\mathbf{D}	\mathbf{E}	\mathbf{F}	\mathbf{G}	Ε	Ι	\mathbf{J}
$ \mathbf{L} $	L	м	Ν	0	Ρ	Q	\mathbf{R}	\mathbf{S}	\mathbf{T}	U	V	W	Х	\boldsymbol{Y}	\mathbf{Z}	А	В	\mathbf{C}	D	\mathbf{E}	\mathbf{F}	\mathbf{G}	Η	Ι	J	\mathbf{K}
\mathbf{M}	\mathbf{M}	Ν	С	\mathbf{P}	Q	R	\mathbf{S}	\mathbf{T}	U	\mathbf{V}	W	Х	\mathbf{Y}	\mathbf{Z}	А	В	\mathbf{C}	\mathbf{D}	E	\mathbf{F}	\mathbf{G}	Η	Ι	J	\mathbf{K}	L
N	Ν	0	\mathbf{F}	Q	\mathbf{R}	\mathbf{S}	Т	U	V	W	х	Y	\mathbf{Z}	А	В	\mathbf{C}	D	\mathbf{E}	F	G	Η	Ι	J	\mathbf{X}	L	\mathbf{M}
0	0	\mathbf{P}	G	\mathbf{R}	\mathbf{S}	\mathbf{T}	U	\mathbf{V}	W	Х	Y	Ζ	А	В	\mathbf{C}	\mathbb{D}	Е	\mathbf{F}	G	Η	Ι	J	Κ	L	М	\mathbf{N}
Ρ	\mathbf{P}	Q	R	\mathbf{S}	Т	U	V	W	х	Y	\mathbf{Z}	А	В	С	\mathbb{D}	Ε	\mathbf{F}	G	Η	Ι	\mathbf{I}	Κ	L	\mathbf{M}	Ν	0
Q	Q	\mathbf{R}	\mathbf{S}	\mathbf{T}	U	v	W	х	Y	Z	А	З	\mathbf{C}	D	\mathbf{E}	F	\mathbf{G}	н	Ι	J	\mathbf{K}	L	\mathbf{M}	Ν	0	\mathbf{P}
\mathbf{R}	\mathbf{R}	\mathbf{S}	T	U	V	W	Х	\boldsymbol{Y}	\mathbf{Z}	А	В	С	D	Ε	\mathbf{F}	G	Η	Ι	\mathbf{I}	\mathbf{K}	\mathbf{L}	\mathbf{M}	Ν	0	\mathbf{P}	Q
S	\mathbf{S}	\mathbf{T}	U	v	W	х	\mathbf{Y}	\mathbf{Z}	А	в	С	D	\mathbf{E}	\mathbf{F}	\mathbf{G}	Η	Ι	J	К	\mathbf{L}	м	Ν	0	P	Q	\mathbf{R}
\mathbf{T}	Т	U	ν	W	Х	\mathbf{Y}	Ζ	Α	В	\mathbf{C}	D	Ξ		\mathbf{G}	Η	Ι	J	\mathbf{K}	L	\mathbf{M}	Ν	0	\mathbf{P}	Q	R	\mathbf{S}
U	U	V	W	х	Y	\mathbf{Z}	А	В	\mathbf{C}	D	E	£	\mathbf{G}	Н	T	J	К	L	\mathcal{M}	Ν	0	\mathbf{F}	Q	\mathbb{R}^{2}	\mathbf{S}	T
V	V	W	Х	\mathbf{Y}	Ζ	A	\mathbf{B}	\mathbf{C}	D	\mathbf{E}	\mathbf{F}	G	Η	Ι	\mathbf{J}	\mathbf{K}	L	\mathbf{M}	Ν	0	\mathbf{P}	Q	R	S	\mathbf{T}	U
W	W	х	\mathbf{Y}	\mathbf{Z}	A	В	С	D	Ε	\mathbf{F}	\mathbf{G}	Η	Ι	\mathbf{J}	\mathbf{K}	L	М	\mathbf{N}	О	\mathbf{P}	Q	\mathbf{R}	\mathbf{S}	Т	U	V
Х	Х	Y	Ζ	А	В	\mathbf{C}	\mathbb{D}	Ε	F	G	Η	Ι	\mathbf{I}	Κ	\mathbf{L}	Μ	Ν	0	Ρ	Q	R	\mathbf{S}	Т	J	V	W
Y	\mathbf{Y}	Ζ	A	В	С	D	\mathbf{E}	\mathbf{F}	G	Η	Ι	l	\mathbf{K}	L	Μ	Ν	0	Ρ	Q	R	\mathbf{S}	\mathbf{T}	U	V	W	х
Ζ	Ζ	A	Е	\mathbf{C}	D	Ε	\mathbf{F}	G	Η	Ι	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	х	\mathbf{Y}

- 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



			A	в	\mathbf{C}	D	Ε	F	G	H	Ι	J	K	L	M	N	0	Ρ	Q	R	S	\mathbf{T}	U	v	w	Х	Y	\mathbf{Z}		
		A	А	В	С	D	Ε	F	G	Η	Ι	J	Κ	2	\mathbf{M}	Ν	0	Ρ	Q	R	S	T	U	V	W	Х	Υ	Ζ		
		B	B	С	С	Ε	F	\mathbf{G}	Η	Ι	\mathbf{I}	Κ	L	\mathbf{M}	Ν	0	Ρ	Q	\mathbf{R}	\mathbf{S}	\mathbf{T}	U	V	W	Х	Y	Ζ	A		
		С	С	D	Ε	F	G	Η	Ι	J	\mathbf{K}	L	\mathbf{M}	Ν	0	\mathbf{P}	Q	\mathbf{R}	\mathbf{S}	Т	U	V	Ŵ	х	Y	Ζ	А	В		
		D	D	\mathbf{E}	F	\mathbf{G}	Η	Ι	\mathbf{J}	Κ	L	\mathbf{M}	Ν	0	Ρ	Q	\mathbf{R}	\mathbf{S}	Т	U	\mathbf{V}	W	х	\mathbf{Y}	Ζ	A	В	\mathbf{C}		
		\mathbf{E}	\mathbf{E}	\mathbf{F}	G	Η	Γ	J	K	L	М	Ν	0	Ρ	Q	\mathbf{R}	\mathbf{S}	Т	U	v	W	х	\mathbf{Y}	\mathbf{Z}	А	З	С	D		
		F	F	Ģ	Η	Т	I.	Κ	T,	М	Ν	0	Ρ	Q	B.	\mathbf{S}	Т	U	V	W	Х	\mathbf{Y}	\mathbf{Z}	A	В	\mathbf{C}	D	E,		
		G	G	\mathbf{H}	Ι	J	\mathbf{K}	L	\mathbf{M}	Ν	0	\mathbf{P}	Q	R	\mathbf{S}	Т	U	V	W	х	\boldsymbol{Y}	\mathbf{Z}	А	В	С	\supset	Ε	\mathbf{F}		
		\mathbf{H}	\mathbf{H}	Ι	J	\mathbf{K}	L	\mathbf{M}	\mathbf{N}	0	\mathbf{P}	Q	\mathbf{R}	5	\mathbf{T}	U	v	W	х	\mathbf{Y}	\mathbf{Z}	Λ	В	\mathbf{C}	D	Ξ	\mathbf{F}	G		
		Ι	Ι	\mathbf{J}	K		\mathbf{M}	Ν	Ο	Ρ	Q	E.	\mathbf{S}	Т	U	V	W	Х	Υ	\mathbf{Z}	A	В	\mathbf{C}	D	Ε	F	\mathbf{G}	\mathbf{H}		
		J	J	\mathbf{K}	\mathbf{L}	$\widetilde{\mathbf{M}}$	\mathbf{N}	0	\mathbf{P}	Q	\mathbf{R}	\mathbf{S}	Т	U	\mathbf{v}	W	х	Y	\mathbf{Z}	А	в	\mathbf{C}	\mathbb{D}	\mathbf{E}	\mathbf{F}	\mathbf{G}	Η	Ι		
		\mathbf{K}	\mathbf{K}	L	\mathbb{M}	Ν	0	\mathbf{P}	Q	R	\mathbf{S}	Т	U	V	W	х	\mathbf{Y}	Ζ	А	В	С	D	\mathbf{E}	\mathbf{F}	G	Е	Ι	J		
Α	R	L M V O P	L M N O D	0 P	NCPG	O P O R c	P OR SE	Q R S T	R S T U	S T J V W		U V W X	V W X V Z	Y Z	X Y Z A B	A	E	A B C D E	B C E F		DEFGH	E F C H	F G H I	G H I J J	H I C K	Ļ	J K H M N	K L M N	0	ĸ
т	н		- 0' rd m {	Q R D T	v d L s 1	T U V W		v V	W X Y Z	X Z Z		A	A B	A B C D F	С	D E	E FE	F G	G F I I I		I	k	K I M N	ИИЛ	M N P	М		N Q R G	C	Ν
Т	Y	Ū X W X	U V W X	V W X V	W X Y Z	X V Z	YZAB		A B C C	E C D E	c	U F G	E F	r F H I	i Co Haria I	н	T	j K L	K L M M	L M N O	M N O P			р Н О Н О Н О Н		*** 55 T T	S V U V	T U V W	С	X
		Y Z	${}_{ m Z}^{ m Y}$	Z A	A E	B C	C D	D E	E F	F G	G H	H I	I J] K	K L			N O		P Q			S T	T U	U V	v w	w x			

- 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)

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

TYBAKZWD

HMWXWXWY

• I replaced by W, W, W

		6	e	1	1	4	4	A	11	14	11	545 25	10		0	13	Tr	4	V	ent:	T	1	1		
a	17	C	1	2	¥.	-	1	2	71	612	i.	R O		64		5 2	tà	11	1	7			È,		
6	e	1	1	2	ŕ	7	2	7	7	-	n	0 0	1		8	-	÷,	F-4	-	4			1 1		
e	d	i	Ż	Ś.	2	2	i	6	21	N7 18	0	pq	T			uv	4		V	2			65		
d	1	1	5	2	7	Ť	1	2	-+-	no	D	9 4				0 10	-	4	Z	8	i l		C A		
e	7	Ľ.	1	2	Ť	6	2	m		0 b	9	7 5	-			y x	4	Z	Ř	a	6	e	1 3	- H	
2	9	1	7	Ť	1	2	-		in the second se	pq		st	4	U	11	x 4	tz	180	a	6	ci	7	e 6		
1	Å	4	Ť	A	7	m	=	0		q r		2 11	4-1-1	W	x	42	-	a	1	c	d	e	5 7	- 1	1
71	1	1	Ż	1	m	n	0	Þ		7 5	t	uv	11	x		2 3	a	6	C	d	e 9	r,	9 8		
i	ī	R	7	20	A	0	p	9		8 Z		UW	x			a a	6	C	ø	e	1	9	6 9		
7	k	1	m	=	0	p	9	T	5	2 11	0	NX	4	Z	8	al	C	d	e	4	9	6	i o	- II	
4	1	-	=	0		9	7	5	2	u v	11	xy	Z	80	R	60	d	e	ø	3	4	i,	i l		
è	30	-	0			7	3		u	11 10	r	4 1	賣	a	6	c d	e	\$	9	A	i,	1	A		
~		0	p	_		5	-			10 %		ZR	a	1	e	1e	8	9	k	i.	1	4	e		
n	0	p			-	- 1	u		-+-	24	¥	-	-	e		2 \$	9	A	1	J	4	1	812		
0	1	9			2			w	-		a		e	2	e	19		i	J	A	1	1	n		
11	9		8	-	u	_	-			Z	f04	be	d	e	1	9 A	i	1	A	1	11	4	0		
it	r		t	-			x			ra	4	cd	e	¥	9	4 i	17	A	1	A	8	0	þ		
Η	8		u				4		8	ab	c	de	1	9	A	17	A	1	m	n	0	10	9		
5	t	-	-		-	4	Z	in t				11	19	ĥ	Zt	14	12	Jan 1	n	0	p	9	r		
	u.		-				-	a			e	19	Th	2	7	iŻ	100	n	0	p	9	r	8		
		W			긝			6		1e		9 h	2	Ż	X I	m	11	0	A	9	r	8	7		
- 4	w	X	4			a	8	c	d	01		hi	V	A	Z	nn	0	p	9	7	5	2	u		
-4	x	4	z	8		1	C	d	el	49	A	ij	A	1	10	1 0	p	9	r	5	t.	а	y		
f	4	7	Ĩ	A	1	C	d	e	6	9 4	6	JA	1	117	n	Op	9		5	2	îl l	U	W		
1	1	ŝ	a	6			e	8	91	66	1	K L	111	n	0	19	7	5	t	u	0		2		
H	Ŷ	a	1			e	1	9	6	iV	K	1 m	n	0	1	9 8	5	10	u	-	-	x	4		
d	a	1	c	_	e	- 44	K4		1	A	2	171 171	0	p	9	r 3	2	u	V	w	z	V	Z		
1	-			-	-				,			7	1		3										
po	SE	e th	e	ke	yw	or	d	to	be	ant	ipo	des	5'	6.5											
i i	t ti	u	a	an	,t	,ie	p'	o d	e	sa	n	t-14	0 0	d	es	ar	ı/t	ip	0	de	S				
Y	phe	red	t	t h	e	m	a	n v	v h	0 5	eı	miı	n d	0	n y	11	t	ue	b	e r	t				
			u	u y	/ y	/ UP	g	5 6	k m	gt	S	t ro	S	S	SI	n j e	m	cu	g	1 1	m				
C	op	y o	ut	the	e c	ýp	he	ree	d ffi	në ti	nus	s. uv	yu	gb	8n	ngts	fro	ss	sn	jen	nci	úĝ	itm		
nt	sei	Sa	re	th	us	16	18	: is	b	1.17	79	8 is	th	us	b	ibq									
	net	the	d	is	ťhi	s																			
Kf	for	t in	th	e 1	st	ve	rtie	cal	col	umn	1, 8	a in	r th	e'i	sť	hon	zo	nta	ál c	ne	, gi	ive	es u		
	6	h.	١.									n .											. 4		
		e .		•	•	• •		•	• •	•	• •	t .		•				•	•			•	· y		
		m	4 :	•	•	•	• •	•	•	• •	• •	i ·				•			•	• •	•	•	····		
		a																							

10	-	17			~										2	-	1		e n									-		-	
AU	1	2	3	4	5	6	2	8		10	"	n	13	14	15	16	5	18	19	20	2	12	22	14	2.5	26.		1	6	57	
at	6	6	d	4	19	1	A	i	1	k	6									a	10	N	2	4	2	8				1	
3	2	d	e.	1	4	A	12	17	I	2	711	n	0	11	9	2	3	ź.	14	u.	4.0	x	4	z	8	4					
e	2	2	1	5	h	i	1	k	2	in	24	0	11	9	1	5	1	en.	v	10	2	Y	2	*	A	6					
10.0	1	5	2	h	i	j	k			n	0	n	9				40.	u	w	z	4	2	¥	a.	6	C	-				
e	¥	3	x	1	i	k	e	272	n	0	11	9	T	3	é	ie	v	10	2	4	2	4	2	6	51	d.		2			
1	19	K.	i	j	k	l	m	n	0	p	9	5	5	t	ú.	v	ed	x	4	z	×	a	4	3	d	4.1	2	N. N.			
2	A	i	;	k	1	m	n	0	n	9	Ŧ	J	t	u	0	N	x	4	2	4	A	6	C	d	4	1		2			
À	ĉ	1	A	6	tra	n	0	n	1	7	5			v		x		x	*	14	6		d	1	1	5.	13	1			
1	5	k	1	m	=1	0	p	9	r	5	1														5	*					Ξ
j	x	2	m	71	0	p	9	7	3	t.	a	v	10	x	4	2	4	а,	6	c	d	e	+	5	A	E.					
k	2	In	-	0	10	9	r	1	t	er	U	14	x	4	2	8	R.	6	e	d	e	1	5	K	i.	j					
1	in	0	0	10	4	Ŧ	5	t	u	0	10	x	4	2	H	a	6	e	d		1	9	h	è	j	k					
in	n	a	12		T	5	2	A	U	w	x	4	z	4	a	6	e	A	e	4	5	A	2	i	k	é					
h	0		4	7	4	1	1	U		x									1		A	i	j	k	e	1.4					
0	p	1	4	1	1	44		-	-	4	•2										2	j	L	1	24	74	1				
12	1.1	1		1		A comments				2								60.00			j.	k	1	In	-	0				_	
4	-	3	1	14			-	-	in the second	y	-	-			-		P. 100	100				2	100	n	0	p					
1	5	C	u		-	1.000	-	- 5-		a		-	-		-			-		k		100	n	e.	p	9					
3	1	4	v	A. Ingen	×					6					-	1.1						71	0	n	1	4					
7	in	U	10	x		2	v	a	6	e				3							71	0	10	9		3					
en	10	10	×	4	2	V	~	6	e	×										24	0	10	1	a.	3	t					
v	0	x	4	2	V	A				e											p	9	r	5	1	ú.					
-	in .	4	2	V	a	6			e	1	9	h	ć	j	k	1	In	11	.0	p	9	7	3	e.	64	0		1			
x	47	2	4	a	6	c	x	2	1		A									9	7	2	t	64	0	6.	1	1		1	
4	2	v.	a	6	4	d	2	3	3	2															4	2					3
2	V				-	-	-	-	k		j														x	7			1		
4		6		d	e	4	3	x	è	i	k	C	In	1	9.	n	9	Ŧ	5	t	da.	0	10	x	7	2			1		
-									-	-		1																			
																			25												

with gft carbo years de makapa zema

the equivalent of the 1st line is taken from the 1st col. from the 2d from 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. with the letter to be cyphered [?] in the 1st column. in the last horizontal line & so on as follows t in the 1st vertical over a in the last horizontal line & so on as follows t in the 1st vertical over a in the last horizontal line & so on as follows t in the 1st vertical over a in the last horizontal line & so on as follows t in the 1st vertical over a in the last horizontal line & so on as follows t in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line & so on as follows f in the 1st vertical over a in the last horizontal line &