Columnar Transposition Cipher

Saturday, February 10, 2024 9:54 AM

Steps

1.) pick out message you want to encrypt:
"Common Sense is not so Common"

2.) Pick key size(can be any number):
"key size you pick will be for how many columns

3.) Draw Columns and fill in with words

1	2	3	4	5	6	7	8
C	O	m	m	O	n	■	S
e	n	S	e	■	i	S	■
n	O	t	■	S	O	■	C
O	m	m	O	n	.		

~~Remember~~ Spaces marked with ■

~~Remember~~ empty left over boxes marked with ↳ ▨

4.) Now mark all of character positions starting from 0 forward excluding the left over boxes

1	2	3	4	5	6	7	8
C	O	m	m	O	n	■	S
0	1	2	3	4	5	6	7
e	n	S	e	■	i	S	■

e 8	n 9	s 10	e 11	[redacted] 12	i 13	s 14	[redacted] 15
n 16	o 17	t 18	[redacted] 19	s 20	o 21	[redacted] 22	c 23
o 24	m 25	m 26	o 27	n 28	. 29		

5.) Now for each box(excluding shaded boxes) do what I do below

1	2	3	4	5	6	7	8
C 0+0=0	O 1+0=1	m 2+0=2	m 3+0=3	o 4+0=4	n 5+0=5	[redacted] 6+0=6	s 7+0=7
e 0+8=8	n 1+8=9	s 2+8=10	e 3+8=11	[redacted] 4+8=12	i 5+8=13	s 6+8=14	[redacted] 7+8=15
n 0+16=16	o 1+16=17	t 2+16=18	[redacted] 3+16=19	s 4+16=20	o 5+16=21	[redacted] 6+16=22	c 7+16=23
o 0+29=29	m 1+29=25	m 2+24=26	o 3+24=27	n 4+24=28	. 5+24=29		

+1 +1

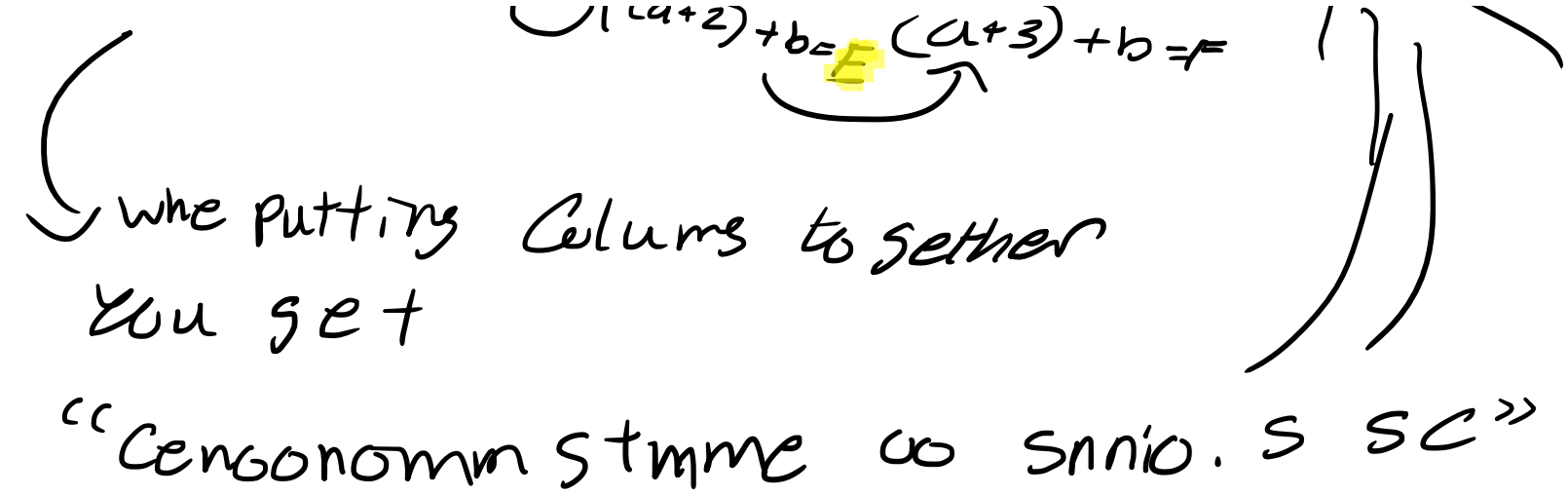
0 → 1 → 2

8 9 10

16 17 18

29 25 26

a+b=C (a+1)+b=D (a+2)+b=E (a+3)+b=F



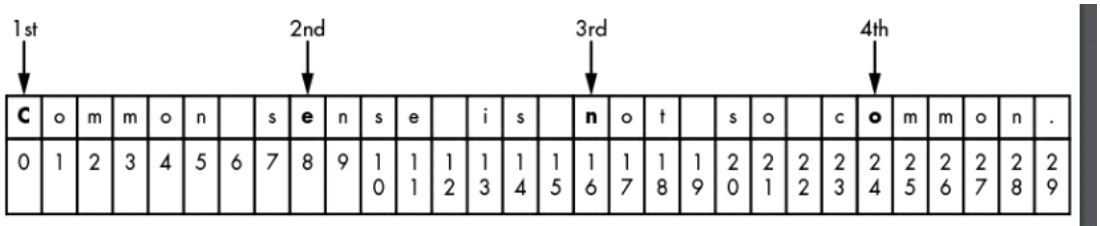


Figure 7-7: Arrows pointing to what `message[currentIndex]` refers to during the first iteration of the for loop when `column` is set to `0`

Although the value in `currentIndex` is less than the length of the `message` string, you want to continue concatenating the character at `message[currentIndex]` to the end of the string at the `column` index in `ciphertext`. When `currentIndex` is greater than the length of `message`, the execution exits the `while` loop and goes back to the `for` loop. Because there isn't code in the `for` block after the `while` loop, the `for` loop iterates, `column` is set to `1`, and `currentIndex` starts at the same value as `column`.

Now when line 36 adds `8` to `currentIndex` on each iteration of line 30's `while` loop, the indexes will be `1`, `9`, `17`, and `25`, as shown in Figure 7-8.

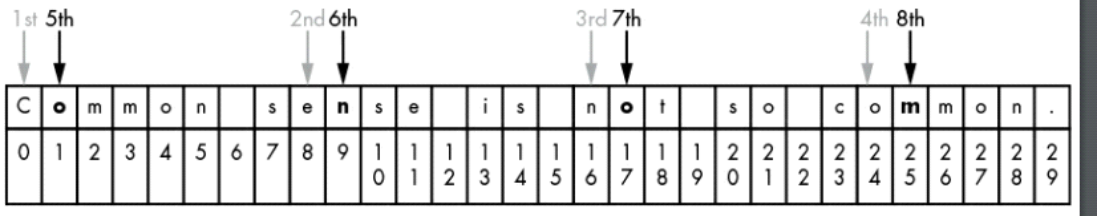


Figure 7-8: Arrows pointing to what `message[currentIndex]` refers to during the second iteration of the for loop when `column` is set to `1`