2.4 Transposition Ciphers

2. Suppose a columnar transposition of 9 columns was used to produce the ciphertext

WLOWA  PELNH  NHLEG  YSOLD  NDWNI
TUEEE  FHDMR  IEBYT  CWEOH  ARRUE.

Decipher the message.

Solution: The problem states that 9 columns were used in the encryption. So we have 5 columns with 6 letters each and then 4 with only 5 letters. Arguably we need to check \( \binom{9}{5} = 126 \) different cases... Let’s start with the assumption that since this is a homework problem the answer is probably going to be one of the first ones we check. So we try the case where the first 5 columns have 6 letters each and the the last four columns only have 5 letters.

W E L L I F I C A
L L E D T H E W R
O N G N U M B E R
W H Y D I D Y O U
A N S W E R T H E
P H O N E

And we get the message: “Well, if I called the wrong number why did you answer the phone?”

4. Encipher COMMON SENSE IS THE BEST DISTRIBUTED COMMODITY IN THE WORLD FOR EVERY MAN IS CONVINCED THAT HE IS WELL SUPPLIED WITH IT using the keyword ALGEBRA.

Solution: There is a difference here in how I taught the material and how the book covers it. Both are valid methods and do not weaken the encryption scheme; they do, however, arrive at different encryptions. I will solve the problem in both ways.

Using my method the keyword is ALGEBRA which has two A’s in it. I ignore the second one and obtain the keyword ALGEBR. This say to write the plaintext in 6 columns:

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

We then write the columns down in the order 1, 5, 4, 3, 2, 6 to get:
Using the book’s method the keyword is ALGEBRA. We don’t ignore the second A we just place it after the first A. In this case we have 7 columns that we order 1, 7, 5, 4, 3, 2, 6. So we take the message and write it in a column of width 7:

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

and then write down the columns in the prescribed order to get:

CEHIT OTDRC EELHS TDUMN LESCW PTOIS
IOYOE NIUW MEERC TWRAV ESDMS BTDIE
OMNHL ETONE SEDHF YODLI INSTB MIRVI
NSPI