1. **Double Transposition Cipher:** Use two keywords to do a tabular transposition cipher twice.

   Encryption Steps

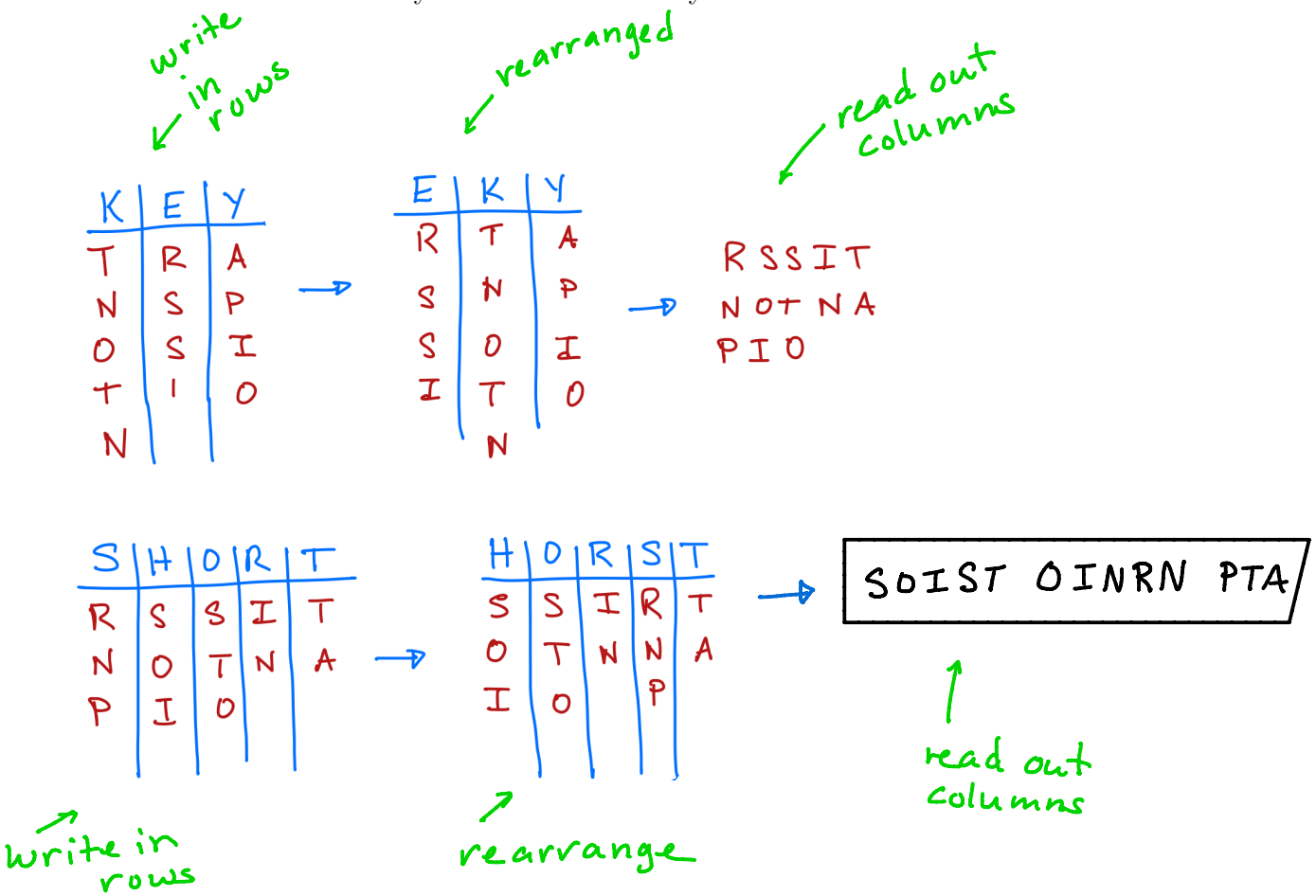
   i. Write the plaintext in **rows** using Keyword 1.

   ii. Rewrite columns with Keyword 1 in alphabetical order.

   iii. Read off the **columns** to form the new "plaintext".

   iv. Repeat this process with Keyword 2.

2. **Example:** Encrypt the word **TRANSPOSITION** using double transposition with Keyword 1: `KEY` and Keyword 2: `SHORT`.



3. How is this different from the tabular transposition with keyword encryption method we used earlier?

   No extra padding.

4. **Decryption:**
   i. Make four grid headers: Keyword 2 (alphabetical order), Keyword 2 (natural order), Keyword 1 (alphabetical order), Keyword 1 (natural order).
   ii. Count the number of characters in the ciphertext and determine grid dimensions.
   iii. Starting with Keyword 2 (alphabetical) grid, fill **columns**.
   iv. Copy columns into the grid for Keyword 2 (natural order).
   v. Read off the **rows** to find new ciphertext.
   vi. Repeat (iii) with Keyword 1 (alphabetical).

SOIST OINRN PTA

5. Decrypt the ciphertext from problem 2. (We know it should decrypt as TRANSPOSITION!)

* pretend like we don't know the answer.

H	O	R	S	T	
S	S	I	R	T	1
O	T	N	N	A	2
I	O		P		

extra

S	H	O	R	T	
R	S	S	I	T	1
N	O	T	N	A	2
P	I	O			

extra

out of rows → RSSIT NOTNA PIO → in columns

E	K	Y	
R	T	A	1
S	N	P	2
S	O	I	3
I	T	O	4
N			

K	E	Y	row
T	R	A	1
N	S	P	2
O	S	I	3
T	I	O	4
N			extra

grid calculation:
letters in cipher text = 13
letters in KEY = 3
letters in SHORT = 5

"KEY" grid: $\frac{13}{3} = 4$ R1 (4 rows w/ 1 extra)

"SHORT" grid: $\frac{13}{5} = 2$ R3 (2 rows w/ 3 extra)

6. Decrypt the ciphertext E T E T S P I H X C R assuming it was encrypted using the scheme above.

grid calculation

letters in ciphertext: 11
letters in SHORT: 5
letters in KEY: 3

"KEY" grid: $\frac{11}{3} = 3$ R2

"SHORT" grid: $\frac{11}{5} = 2$ R1

H	O	R	S	T
E	E	S	I	C
T	T	P	H	R
			X	

into cols.

S	H	O	R	T
I	E	E	S	C
H	T	T	P	R
X				

out of rows → IEESC HTTPR X → into cols

E	K	Y
I	C	P
E	H	R
E	T	X
S	T	

K	E	Y
C	I	P
H	E	R
T	E	X
T	S	

out by rows

CIPHERTEXTS