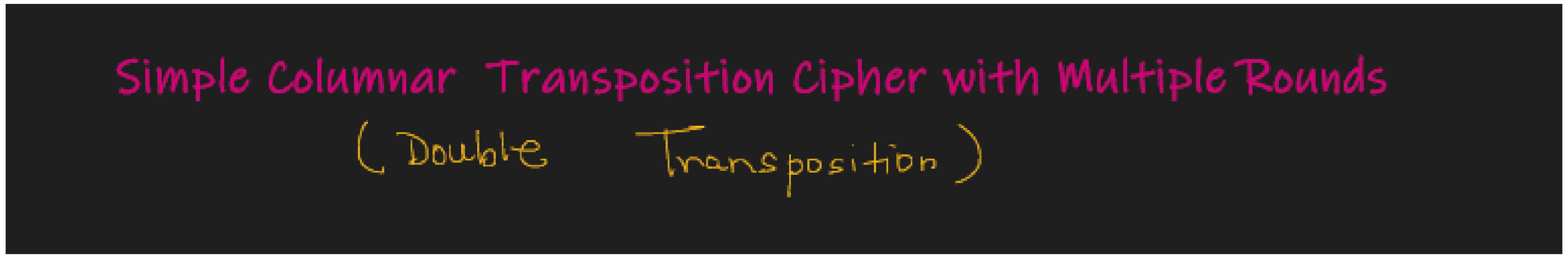
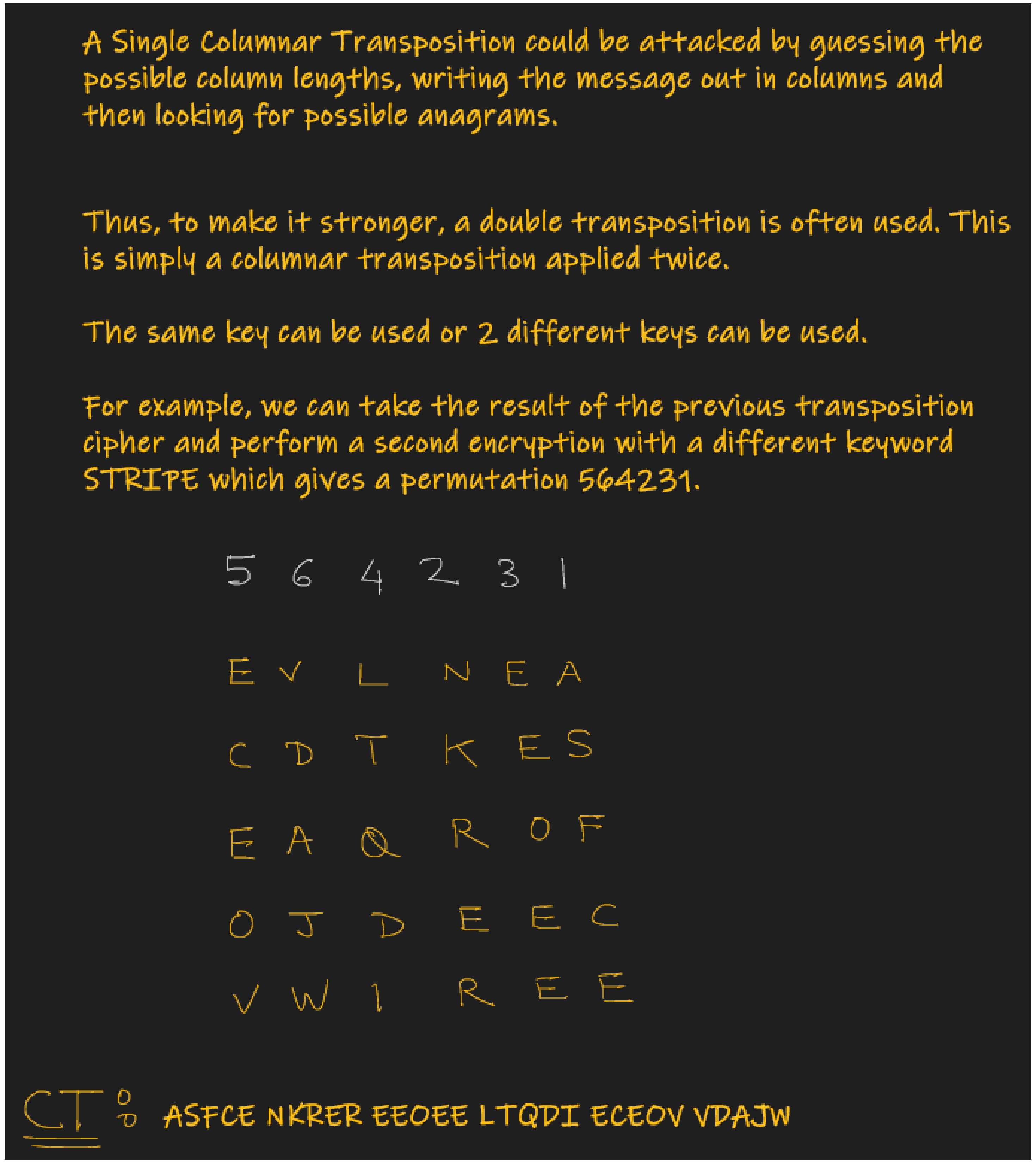


Simple Columnar Transposition Cipher with Multiple Rounds

(Double Transposition)



A Single Columnar Transposition could be attacked by guessing the possible column lengths, writing the message out in columns and then looking for possible anagrams.

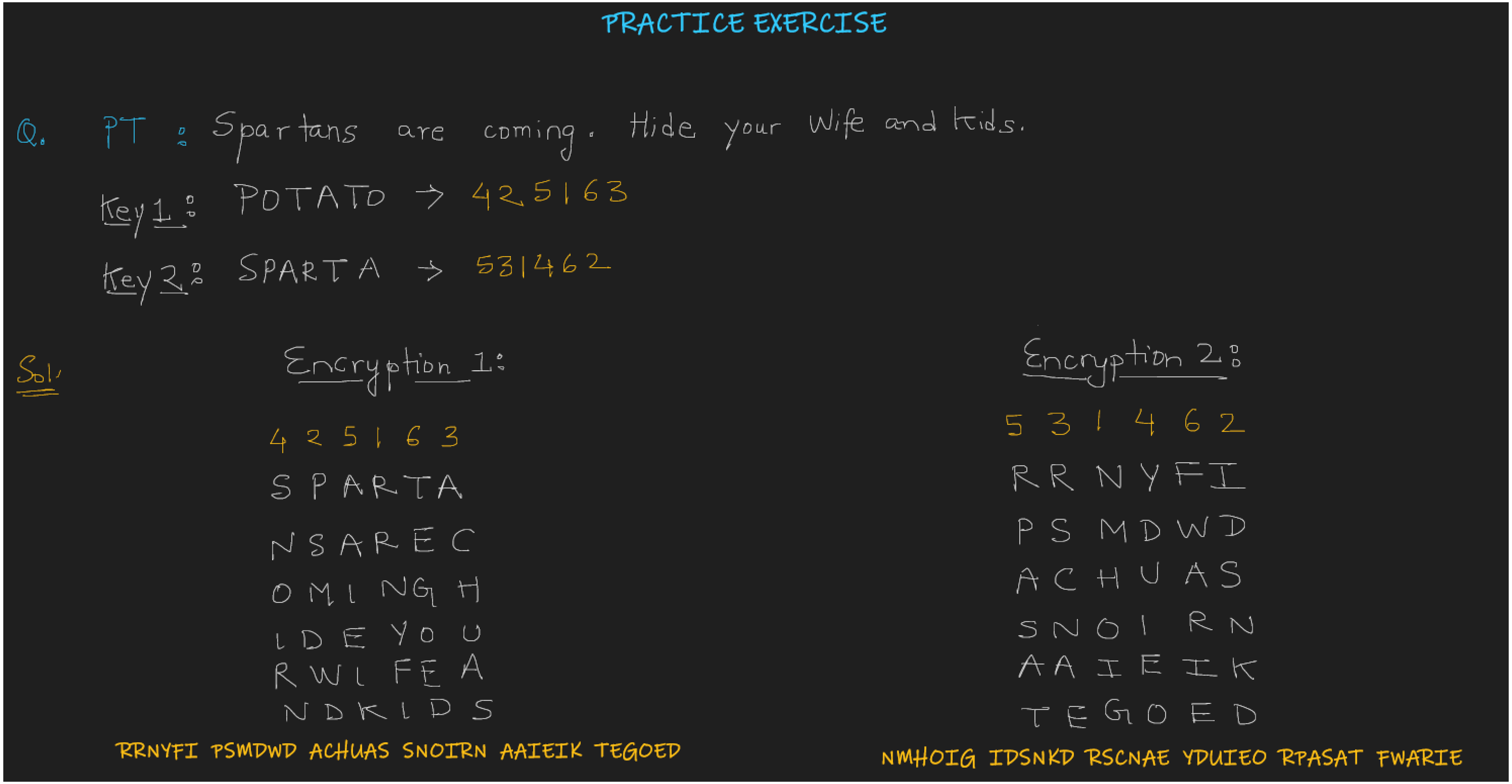
Thus, to make it stronger, a double transposition is often used. This is simply a columnar transposition applied twice.

The same key can be used or 2 different keys can be used.

For example, we can take the result of the previous transposition cipher and perform a second encryption with a different keyword STRIPE which gives a permutation 564231.

5	6	4	2	3	1
E	V	L	N	E	A
C	D	T	K	E	S
E	A	Q	R	O	F
O	J	D	E	E	C
V	W	I	R	E	E

CT : ASFCE NKRER EEOEE LTQDI ECEOV VDAJW



PRACTICE EXERCISE

Q. PT : Spartans are coming. Hide your Wife and Kids.

Key 1 : POTATO → 425163

Key 2 : SPARTA → 531462

Sol.

Encryption 1:

4	2	5	1	6	3
S	P	A	R	T	A
N	S	A	R	E	C
O	M	I	N	G	H
I	D	E	Y	O	U
R	W	I	F	E	A
N	D	K	I	D	S

RRNYFI PSMDWD ACHUAS SNOIRN AAIEIK TEGOED

Encryption 2:

5	3	1	4	6	2
R	R	N	Y	F	I
P	S	M	D	W	D
A	C	H	U	A	S
S	N	O	I	R	N
A	A	I	E	I	K
T	E	G	O	E	D

NMHOIG IDSNKD RSCNAE YDUIEO RPASAT FWARIE