

1. Review **shift ciphers**: What is the key in the shift cipher below? KEY: 11

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
in	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
out	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

2. A shift cipher is a particular type of **substitution cipher**. Below is a substitution cipher that is **not** a shift cipher.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
in	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
out	E	F	G	L	8	A	R	Q	T	U	V	P	B	D	N	O	H	M
	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
in	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9
out	i	1	4	7	J	6	5	K	9	3	2	0	C	X	S	Z	Y	W

(a) Encrypt: MEET APRIL 3

B881 EPMTPO
 ↑ zero

(b) Decrypt: F4IE19Z09

BUSAT0730
 Bus at 07:30

(c) What key is needed to decrypt a message using this encryption scheme?

You need the entire substitution grid

(d) Which substitution is, in general, harder to break, a shift cipher or one that is not a shift cipher?

non-shift substitutions are much harder!

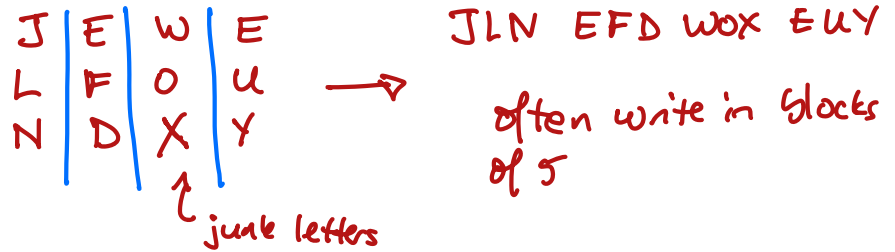
(e) What strategies would you use to try to break a substitution cipher that is not a shift cipher?

Look for repeated letters in the ciphertext - if it's encrypted with a substitution they will always represent the same letters in the plaintext. ← Frequency Analysis lets you guess common letters!

3. Another encryption scheme is called a **transposition cipher**.

Encode JEWEL FOUND using a transposition cipher of rows of 4 letters (4 columns).

- (a) Put in rows
- (b) read out columns



4. Decrypt

BNEAA ANBDA RX

JLNEF DWOXE
UY

if it was encoded with a transposition cipher with rows of 4 letters (4 columns).

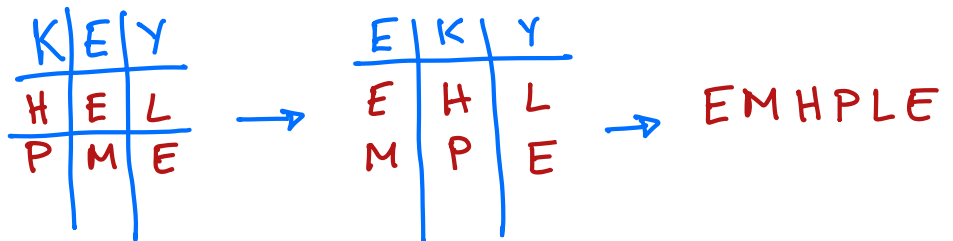
- (a) How many rows? 12 letters and 4 letters/row ⇒ 12/4 = 3 rows
- (b) Put in columns
- (c) read out rows



5. Encrypt using a transposition cipher with a keyword KEY:

HELPM E

- (a) Put in grid by rows
- (b) Mix up columns
- (c) Read out columns



6. Decrypt using a transposition cipher with a keyword KEY:

FNTIU IODX ← 9 letters

- (a) Determine how many rows 9/3 = 3 ⇒ 3 rows
- (b) Put in grid by **columns**, labeled by SORTED keyword
- (c) un-mix-up columns
- (d) Read out **rows**

