Summary packet for Junior Cryptorally

1. Shift

1.1. **Decoding.** To decode a message.

(1) Find the additive inverse of the key.

(2) Change each letter to a number using the translation table.

(3) Either **subtract the key** or **add the additive inverse of the key** to each number. Do whichever is easier, you get the same result.

(4) Change each number back to a letter using the translation table.

1.2. **Example.** Let's decode HVSEIWQYPFCKBTCLXIADGCJSFHVSZONMRCU, which was ENCODED with 14

(1) Find the additive inverse of 14, which is 12, since 26-14=12.

(2) Change each letter to a number using the translation table.

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

(3) Either subtract 14 or add the additive inverse of 12 to each number.

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

(4) Change each number back to a letter using the translation table.

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

So the original message was

THEQUICKBROWNFOXJUMPSOVERTHELAZYDOG

2. Vigenère

2.1. **Decode.**

(1) Change each letter in the **key word** to a letter and then *w*rite down the additive inverse in mod 26 of each number. Write this down off to the side.

(2) Change each letter in the message to a number.

(3) Underneath the message in numbers, write down the inverse key in numbers. Repeat the inverse key enough times to have a number under each number in the message.

(4) Add the number in the message to the number from the key below it. Remember to use the mod 26 system.

(5) Change each number in the result back to a letter.

2.2. **Example.** Let's decode "XEVRBETYPSLNECM", which was ENCODED with the key "rain".

(1) "rain" is 17 0 8 13, whose additive inverse is 9 0 18 13.

(2) "XEVRBETYPSLNECM" becomes 23 4 21 17 1 4 19 24 15 18 11 13 4 2 12.

(3) Now I repeat 9 0 18 13 enough times to fill up the whole message.

X	E	V	R	B	E	T	Y	P	S	L	N	E	C	M
23	4	21	17	1	4	19	24	15	18	11	13	4	2	12.
9	0	18	13	9	0	18	13	9	0	18	13	9	0	18

(4) Now add them.

X	E	V	R	B	E	T	Y	P	S	L	N	E	C	M
23	4	21	17	1	4	19	24	15	18	11	13	4	2	12.
9	0	18	13	9	0	18	13	9	0	18	13	9	0	18
6	4	13	4	10	4	11	11	24	18	3	0	13	2	4

(5) Now translate back to letters.

X	E	V	R	B	E	T	Y	P	S	L	N	E	C	M
23	4	21	17	1	4	19	24	15	18	11	13	4	2	12.
9	0	18	13	9	0	18	13	9	0	18	13	9	0	18
6	4	13	4	10	4	11	11	24	18	3	0	13	2	4
G	E	N	E	K	E	L	L	Y	S	D	A	N	C	E

Our decoded word is GENEKELLYSDANCE.

3. Affine

3.1. **Decode.** The key is two numbers.

(1) Change all the letters in the encoded message to numbers.

(2) Find the additive inverse of the second number in the key.

(3) **Add the additive inverse** of the **second** number in the key or **subtract the second number** in the key to each number in the encoded message. Add the inverse or subtract the key, whichever is easier, you get the same result. You can use the orange addition table to do the addition.

(4) Find the multiplicative inverse of the first number in the key. You can use the multiplicative inverse table.

(5) **Multiply by the multiplicative inverse of the first number** in the key or **divide by the first number** in the key. You can only divide if the number you are dividing into is a multiple of the first number in the key. You can use the purple multiplication table for the multiplication.

(6) Change all the numbers back to letters.

3.2. **Example.** We receive the coded message IBCIGHXOOUU and we know it was encoded with (3,2).

(1) The first number of the key is 3. The multiplicative inverse of 3 is 9, since $3 \times 9 = 1$ in our mod 26 number system.

(2) The second number of the key is 2. The additive inverse of 2 is 24, since 2+24 = 0 in our number system. (26-2=24)

(3) As usual, change each letter to a number.

I	B	C	I	G	H	X	O	O	U	U
8	1	2	8	6	7	23	14	14	20	20

(4) Now we add 24 (subract 2) to each.

I	B	C	I	G	H	X	O	O	U	U
8	1	2	8	6	7	23	14	14	20	20
-2	+24	-2	-2	-2	-2	-2	-2	-2	-2	-2
6	25	0	6	4	5	21	12	12	18	18

(5) Now we multiply by 9 (divide by 3) to each.

I	B	C	I	G	H	X	O	O	U	U
8	1	2	8	6	7	23	14	14	20	20
-2	+24	-2	-2	-2	-2	-2	-2	-2	-2	-2
6	25	0	6	4	5	21	12	12	18	18
÷3	×9	÷3	÷3	×9	×9	÷3	÷3	÷3	÷3	÷3
2	17	0	2	10	19	7	4	4	6	6

(6) Finally change back to letters.

I	B	C	I	G	H	X	O	O	U	U
8	1	2	8	6	7	23	14	14	20	20
-2	+24	-2	-2	-2	-2	-2	-2	-2	-2	-2
6	25	0	6	4	5	21	12	12	18	18
÷3	×9	÷3	÷3	×9	×9	÷3	÷3	÷3	÷3	÷3
2	17	0	2	10	19	7	4	4	6	6
C	R	A	C	K	T	H	E	E	G	G

The message was CRACKTHEEGG.

4. Railfence

4.1. **Decode.** You are given a coded message and the key.

(1) Make the zig-zag pattern with the same number of boxes as the number of letters in the message you received. The number of lines in each zig-zag is the key.

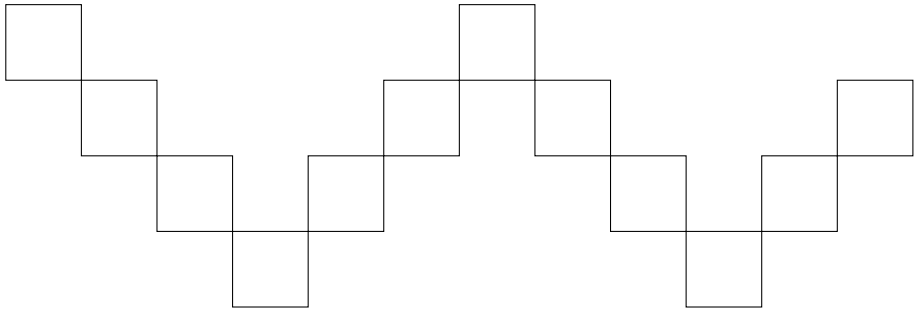
(2) Fill in all the peak-boxes of the zig-zag with the first letter of the message. Cross the letters out as you use them.

(3) Fill in all boxes of the second row of the zig-zag with the next letters of the message. Cross the letters out as you use them.

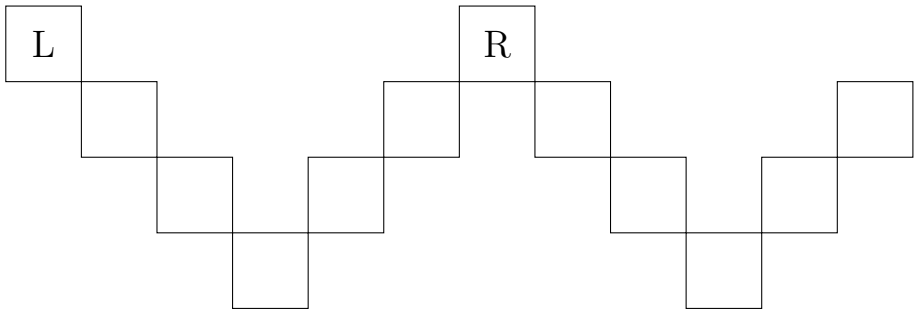
(4) Keep going until all the letters are gone and all the boxes filled. Now read along the zig-zag.

4.2. **Example.** You receive the mesage LREEANTHTUTR, which was encoded with key 4.

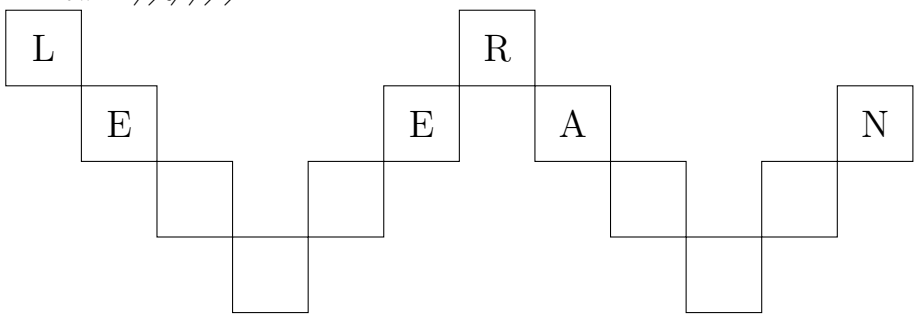
(1) The message has 12 letters, so make a zig-zag of 12 boxes, depth 4.



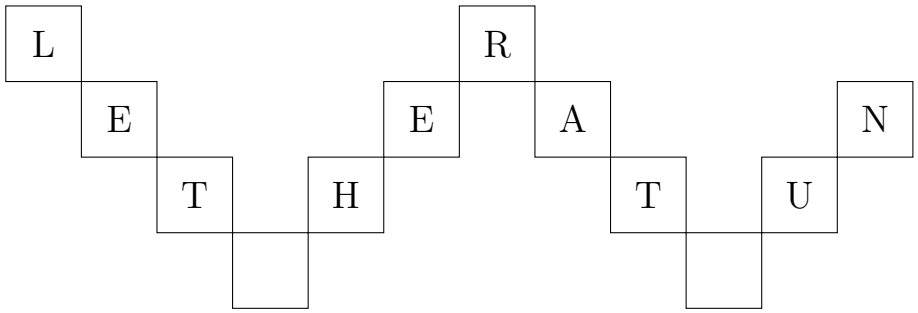
(2) Fill in the peaks. ~~L~~~~R~~EEANTHTUTR



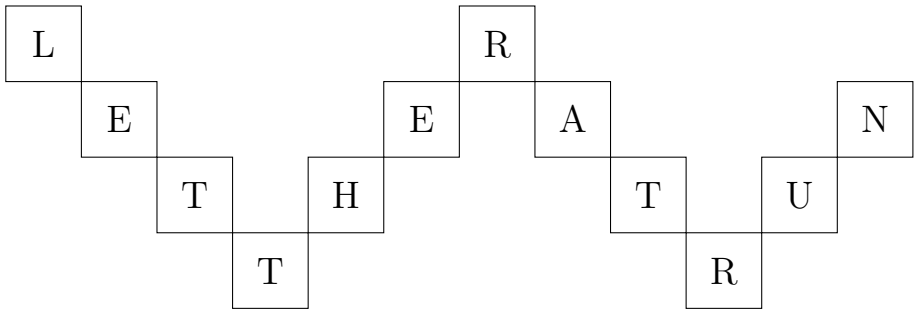
(3) Fill in row 2. ~~L~~~~R~~~~E~~~~E~~~~A~~N



(4) Fill in row 3. ~~LREEANTHTU~~TR



(5) Fill in row 4. ~~LREEANTHTUTR~~



The original message was LETTHERATRUN

5. Playfair

5.1. **Decoding.** To decode, we need a coded message and a key. The key for playfair is a word.

Step 1: Prepare the key array: Delete all duplicate letters in the key and any 'j' in the key. Now add the the rest of the alphabet after your message. You have 25 letters: arrange these in a 5 by 5 grid and let i and j share a spot as i/j.

Step 2: Prepare the message: Break the message up into pairs, in order. You should never have a pair with of the same letter. If you do, then check your pairs.

Step 3: Decode the pairs: Each pair is decoded separately.

- If the two letters in the digram both appear in the same column of the encryption grid, each letter of the pair is replaced with the letter immediately **above** it in the grid. If there is no letter above, use the letter from the bottom of the same column.
- If the two letters in the digram both appear in the same row of the encryption grid, each letter of the pair is replaced with the letter immediately to its **left** in the grid. If there is no letter to the left, use the the last letter in the row.
- If the two plaintext letters in the pair are neither in the same row nor in the same column of the encryption grid, each is replaced by the letter in its own row that shares a column with the other letter of the pair.

5.2. **Example.** Let's decode hegilxbhlaubedunedunedrv, which was encoded with key=theeggandi.

(a) Remove all the duplicates from theeggandi. It becomes thegandi.

(b) Add the rest of the alphabet. Now we have thegandibcfklmopqrsuvwxyz.

(c) Arrange in a five by five grid.

t	h	e	g	a
n	d	i/j	b	c
f	k	l	m	o
p	q	r	s	u
v	w	x	y	z

(d) Arrange hegilxbhlaubedunedunedrv in pairs.

he
gi
lx
bh
la
ub
ed
un
ed
un
ed
rv

(e) Decode the pairs.

he	$\rightarrow$	th
gi	$\rightarrow$	eb
lx	$\rightarrow$	ir
bh	$\rightarrow$	dg
la	$\rightarrow$	oe
ub	$\rightarrow$	sc
ed	$\rightarrow$	hi
un	$\rightarrow$	pc
ed	$\rightarrow$	hi
un	$\rightarrow$	pc
ed	$\rightarrow$	hi
rv	$\rightarrow$	px

(f) The message is thebirdgoeschipchipchip

6. Practice examples

(a) Decode LWHLJDQZCRTGPJZFCPYPXTPDYZESTYRLYYZJDESPXDZXFNS, which was ENCODED by shift, key 11.

(b) Decode UWWIQBQTVEHBKDSX, which was ENCODED by shift, key 16.

(c) Decode IBWTCIIPXMZLFZ, which was ENCODED by Vigenère, key PUSHOVER.

(d) Decode UVEHTHRBDVRNOGQNJSTEZ, which was ENCODED by Vigenère, key BOAT.

(e) Decode MHCZKJMBBI, which was ENCODED by affine, key (7,8).

(f) Decode ODEFWNOTTE, which was ENCODED by affine, key (11,4).

(g) Decode FTLPIDHPAYUNETS, which was ENCODED by railfence, key 3.

(h) Decode ASULITORRWLEYMEASNOOHYTT, which was ENCODED by railfence, key 5.

(i) Decode NGGTFDFEPAKQPABEVY, which was ENCODED by playfair, key TWEEDLEDUM

(j) Decode YNHQGPFIGXDAKGYNFVOMSQXAXGECRBSBMLFLSGTBYNHPMX, which was ENCODED by playfair, key DODO