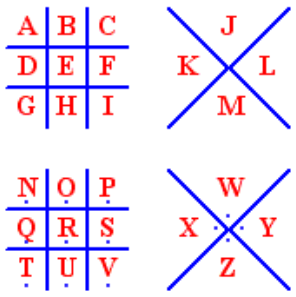
Meeting 4: Fun with Ciphers!

October 21, 2012

1. Pigpen Cipher



(a) Encode the following message using the Pigpen cipher:
GOOD AFTERNOON

(b) Decode the message written using the Pigpen cipher:

(c) Write your own message to your partner using this cipher, and see if they can decode it!

Encoded message:

Decoded message:

2. Encoding with the Rail Fence Cipher

(a) Encode the phrase WE NEED YOUR HELP using the Rail Fence cipher

i. First, make an outline of the zig-zag pattern for the number of letters that are in your message

(WE NEED YOUR HELP has 14 letters)

_				_				_				_	
	_		_		_		_		_		_		_
		_				_				_			

ii. Arrange the letters of the message on the zig-zag pattern:

W				E				U				L	
	E		E		D		O		R		E		P
		N				Y				H			

iii. Then, the encoded phrase is written out left-to-right, top-to-bottom. This time, we have also devided the message into three "words" (each word has letters written on one of the lines above)

WEUL EEDOREP NYH

(b) Use the Rail Fence cipher to encode the message

I WILL BE THERE SOON

_				_				_				_			
	_		_		_		_		_		_		_		_
		_				_				_				_	

What will the encoded text read?

3. **Decoding Rail Fence Cipher**

(a) If the message is divided into 3 "words", you can simply read off the message as follows:

i. Write down the *first* letters of each of the words number 1, 2 and 3

ii. Then, write down the *second* letters of each of the words 2, 1 and the third letter of 2 (watch out for the order!!!)

A. If you notice the order, you are constantly oscillating between 1, 2, 3, 2, 1, 2, 3...

iii. Continue writing the next letters switching between the two patterns.

For example, here is how one can decode the message we encoded above:

iv. Decode the message below using this method (it was encoded using the Rail Fence cipher):

TTNY IEOUAA MRW

(b) If the message is *not* divided into three "words", decoding gets more complicated. Here is what you need to do:

i. Count the number of letters in the message.

ii. Make an outline of the zig-zag pattern like we did above for the number of letters in the message.

iii. Fill in the top row first (fill in letters into the boxes with underlined spots only)

iv. After that fill in the middle row

v. Finally, fill in the third row

vi. Read the message, inserting spaces where necessary

(c) Decode the following message that was encoded with the Rail Fence cipher:

IEHTLVMTEAISOAMC

i. How many letters are there in the message?

ii. Count the number of underlined spaces. Is it equal to the number of letters in the message? If so, put the letters into the decoding outline below:

_				_				_				_			
	_		_		_		_		_		_		_		_
		_				_				_				_	

iii. Write out the encoded message below:

4. Greek Square Cipher

(a) A famous historian and cryptographer, named Polybius, invented the Greek Square Cipher 2,200 years ago:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

i. Each letter in the alphabet is replaced by a two digit number corresponding to its position in the square matrix. The *Row Number* is in front of the *Column Number*. For example,

- the letter M is encoded by 32;
- the word MATRIX is encoded by 321144422453;

ii. Find the two digit numbers that correspond to the following letters:

$$n =$$
$$r =$$
$$i =$$
$$j =$$

iii. Do you think it is a problem that both i and j are encoded by the same number? Explain.

iv. Decipher the following messages. (The first message has separated into two digit numbers to help you with the encoding. The second one is more challenging)

- **24 11 32 42 45 33 33 24 33 22 11 52 11 54**

- **333432154343112215 43**

5. **Vigenère Cipher**

Below is a Vigenère Cipher:

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	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
L	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
M	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	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

6. Let's figure out how this table is constructed:

   (a) Take a look at row labeled A. How is it related to the alphabet?

   (b) How is row C obtained from the alphabet?

   (c) How is row Z obtained from the alphabet?

   (d) What can you say about all of the rows? Explain to the teacher at your table how this table is made. Once you are done with that, you are ready to use the Vigenère to encode messages!

7. Here is how encoding with the Vigenère cipher works:

(a) First, choose a *keyword*. The keyword should be known to the encoder and the reciever of the message. It is kept secret from everyone else. For example, we will use the keyword CAR. The keyword tells you which rows to use in the encoding.

(b) Then, select the message you want to send. For example, the message can say: UNDERATTACK

(c) Repeat the keyword enough times to get the length of the message. For example, UNDERATTACK is a message consisting of 13 letters. The repeated keyword will look as follows:

CARCARCARCA

(d) Finally, we are ready to encode. In this example, we will only use three rows (C, A and R).
To encode, write down the repeated keyword under the message:

message:	**U**	**N**	**D**	**B**	**R**	**A**	**T**	**T**	**A**	**C**	**K**
repeated keyword:	C	A	R	C	A	R	C	A	R	C	A
encoded message:	**W**	**N**									

For each letters in the message, the letter in the repeated keyword tells you which wor you need to use for encoding.
For example, to encode the first letter of the message (**U**), use row C. The encoded letter will be W.
Incode. In the same way, to encode the second letter of the message (**N**), use row A. The encoded letter will be A.

(e) Next, is to encode the text. First, we find Row C, then we identify Column U. The first encoded letter is W because this is where these two cross. Next we look for Row A and Column N to get the next encoded letter, N.

Encode the rest of the message into the table above.

(f) Knowing that the keyword is CAR, decode the following message:

IOFFJFDTYCTNCSYCRF

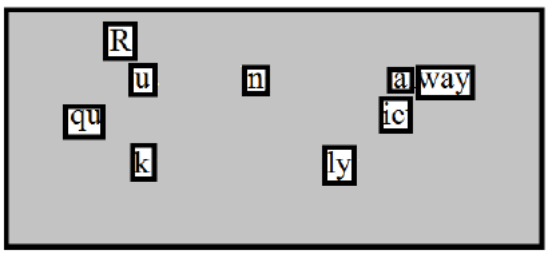
Use the table below to help you organize your thoughts:

message																		
repeated key word	C	A	R															
encoded message	**I**	**O**	**F**	**F**	**J**	**F**	**D**	**T**	**Y**	**C**	**T**	**N**	**C**	**S**	**Y**	**C**	**R**	**F**

8. **Cardan Grille** In this method of encoding, a message is hidden within a larger text, and the key to decoding it is a grid with cutouts that reveal the letters of the actual message.

(a) Below is a message that appears to be a letter from someone named Alice to her Cousin Ralph. After looking at it using the attached grid, it reveals a hidden message.

Cousin Ralph,
I hope you are doing well, as always. I was quite impressed by the pictures you sent, thank you. Hopefully we will see you soon.
-Alice



What is the letter really telling the reader?

(b) Sometimes the message is hidden within other words. Use the grille you brought to decode the message hidden in the words below:

A	F	J	T	A	V
I	F	N	E	K	L
Q	T	P	L	A	X
D	H	S	V	B	T
I	R	C	C	F	E

(c) Notice that the surrounding letters do not need to be really meaningful. Now try making your own message for your partner with the grille you made.
