CRYPTO I: CREATING–AND CRACKING–CODES AND CIPHERS

MATH CIRCLE (BEGINNERS) 01/15/2012

1. Caesar Cipher

Before Julius Caesar was Emperor, he was a General in the Roman Army. He needed to send secret messages to other generals, but he was worried that the soldier carrying the messages might be caught by the enemy. So he would encrypt them by shifting the letters of the original message by a certain amount.

For instance, with a shift of +3 (also known as an a-D shift), a $\rightarrow$ D, b $\rightarrow$ E, c $\rightarrow$ F, and so on. When you get to the end of the alphabet, it wraps around, so x $\rightarrow$ A, y $\rightarrow$ B, and z $\rightarrow$ C. The value "3" is the key for this version of the Caesar Cipher, and it gives a codetable (a chart that helps with encrypting and decrypting) that looks like this:

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
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

(1) What are the different possible keys (shifts) for a Caesar cipher? How many are there?

(2) Encrypt the message "attack at dawn" using a Caesar cipher with a shift of your choice:

Shift value:

Ciphertext (encrypted message):

a	t	t	a	c	k		a	t		d	a	w	n

(3) The following riddles have answers encrypted with a Caesar cipher. Can you figure out the answers? HINT: Try to make a good guess about what the shift is, then you won't have to try lots of keys before you get the answer.

(a) What do you call a dog at the beach?

E L S X H S K.

(b) Three birds were sitting on a fence. A hunter shot one. How many were left?

V W V M. B P M W B P M Z A N T M E

I E I G.

(c) What animal keeps the best time?

K G K D M R N Y Q.

(4) The Italian Mafia boss Bernardo Provenzano used a secret code similar to the Caesar cipher to hide the names of his associates in messages. He was captured in 2006, in part because the police broke his cipher. Here is one example of something he actually wrote (except he wrote it in Italian):

"I met **5,12,15,15,22 19,12,12,15,4** and we agreed that we will see each other after the holidays."

The Italian alphabet has fewer letters than the English alphabet–it's missing J, K, W, X, Y. You can use the following Italian-style codetable to help you:

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

Can you help the police crack the code and figure out the name of Provenzano's associate?

2. KEYWORD CIPHERS

Caesar ciphers are not very secure. Someone who wants to crack them only needs to try 25 different possibilities for the key! Caesar ciphers are an example of a more general type of cipher known as a *(monoalphabetic) substitution cipher*. This means that each letter of the plaintext alphabet is always transformed to a specific letter in the ciphertext. Another kind of substitution cipher is a *keyword cipher*. Here's how they work:

- Find a friend with whom you'll want to exchange secret messages. Agree on a secret keyword, for instance "DOG", and a secret key letter, for instance "H". If your keyword has any repeated letters, use only the first of each one. For example, the keyword "APPLES" would become "APLES" and "BANANAS" would become just "BANS".

- Write down the alphabet in lowercase–these represent plaintext letters. Starting just below the key letter, write the keyword, then continue with the remaining letters of the alphabet. Be sure to skip the letters you already used in the keyword, when you get to them in the alphabet!

Example: The keyword DOG and key letter H gives a codetable that looks like this:

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

5) With a partner, create a keyword cipher and fill in the the encoding/decoding table below.

KEYWORD:

KEY LETTER:

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

Use your table to encode:

(1) “the hideout is not safe”

(2) “meet me at six pm”

(3) any message you like! When you’re done encoding it, transfer the ciphertext to another sheet of paper and have your partner decrypt it using their codetable.

3. Frequency Analysis

Now let's try to break keyword ciphers. Each group will get a different piece of plain English text to analyze.

Work together to count the number of times each letter appears in your text:

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency													

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency													

(This table is not like the others so far–it won't be used to encrypt or decrypt messages, it's just used to keep track of how often each letter occurs.)

When each group is done, we'll combine the answers to get an overall idea of how frequent each letter is in English.

3) Now try to decrypt this text, which uses a keyword substitution cipher. The first step is to count the frequency of each letter–work together to do this more quickly!

F U R H J U F E P Q J I K Q J O J N W X E N J

K O C R W P N Q J N F R I X W J H F W K

G J U R J Y J R V Z X N N R G U J K Q R W P N R

I F O J N F C C X E Q F Y J W K Q F I V E H Q

Z O F H K R H J N F R I K Q J M E J J W A Q J W R

A F N C X E W P J O R F U A F C N I R I R K L X O

Q F U L F W Q X E O F I F C A Q C N X V J K R V J N

R Y J G J U R J Y J I F N V F W C F N N R B

R V Z X N N R G U J K Q R W P N G J L X O J

G O J F T L F N K – U J A R N H F O O X U U L O X V

F U R H J R W A X W I J O U F W I.

#1

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency													

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency													

#2

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency													

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency													

#3

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency													

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency													

#4

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency													

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency													

#5

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency													

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency													