JUNE 13TH CRYPTOGRAPHY PROBLEM SET

Those who can imagine anything, can create the impossible.– Alan Turing

We are going to learn about two more ciphers. Autokey and general substitution ciphers. We begin with autokey, which is a variant of the Vigenére cipher. In fact, Vigenére did not invent the Vigenére cipher, he invented Autokey.

The idea is quite simple. It begins just like a regular Vigenére cipher, but instead of repeating the code word over and over, it repeats the ciphertext.

f	r	o	g	s	a	l	l	y	o	u	r	b	a	s	e	a	r	e	b	e	l	o	n
5	17	14	6	18	0	11	11	24	14	20	17	1	0	18	4	0	17	4	1	4	11	14	13
a	l	l	y	o	u	r	b	a	s	e	a	r	e	b	e	l	o	n	g	t	o	u	s
F	C	Z	E	G	U	C	M	Y	G	Y	R	S	E	T	I	L	F	R	H	X	Z	I	F

1. Figure out how to decrypt using autokey. Then decrypt the following message (the spaces should be ignored.

`EOFL LWYI LQFM KCLM XODX TEYH KRBK HHFC PYFA VXSL FHW`

There are some tables that can help with this.

2. Encrypt a message using autokey. It should be about three lines long on the included tables. We will share these messages with other teams and have a race to see which team can decrypt fastest.

Now we will talk about substitution ciphers. This is a simple idea. For each letter in the alphabet, we are going to turn it into a different letter. For instance we could do:

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

3. I encrypted a phrase using the adjacent substitution cipher. Decrypt it.

```
OYQD QFLV OZWT VQFR TKOF USTZ IODL ZXRN ZITD QZIT DQZO EL
```

4. How many different substitution ciphers are there? Do you think it is possible to brute force it like we did for Caesar shift (just try all possible encryptions?)

5. Suppose I give you a long string of text that was encrypted using a general substitution cipher. How would you break it? (You need to do more than analyze which letters are most common). We'll try to implement some tools to help with this on Thursday afternoon.

6. Discuss with your group how to make a general substitution cipher even more resistant to this sort of attack.