JUNE 7TH CRYPTOGRAPHY PROBLEM SET

There is no castle so strong that it cannot be overthrown by money. – Cicero

We are going to learn about Vigenére ciphers, this was the the le chiffre ind echiffrable (the indecipherable cipher) until the middle of the 19th century. It was still in use during the American civil war.

Vigenére ciphers are Caesar shifts, but different letters have different shifts.

Here is an example that we also did on the board.

f	r	o	g	s	f	r	o	g	s	f	r	o	g	s	f	r	o	g	s	f	r	o	g
5	17	14	6	18	5	17	14	6	18	5	17	14	6	18	5	17	14	6	18	5	17	14	6
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	Z	I	P	G	K	J	R	F	K	T	J	C	C	T	Y	Y	F	I	Y

1. I encrypted the following text using the code word `CAT`. What did I really say?

`GVXT YWQG LCYL YOHH`

2. Break up your team into groups of 2 people. Encrypt a message and send it to the other two people. You can use the attached sheet for doing the work. Write your plaintext below. Write your decrypted ciphertext (from the other pair team members) here. Make sure to check your answer. If you have time, send a message to another group.

Next, we will learn about columnar transposition, this is another kind of cipher which was still in regular use in World War I and World War II. We start with an example.

C[2]	A[1]	T[3]
t	h	e
e	n	e
m	y	f
o	r	c
e	s	a
r	e	h
e	r	e

We read vertically down the A column first, since that's the first letter in the word, alphabetically. Then we read down the C column and finally down the T column. This gives us the cipher text.

hnyrsertemoereeefcahe

If there are open spots, fill them with random letters, like in the Scytale.

3. Encrypt the phrase "MODULAR ARITHMETIC IS FUN" using the keyword MATH. You can use the included tables to help.

4. I encrypted a phrase using the keyword GAME. I obtained the following ciphertext.

"AMCTUOAWHTIEIROFMEISMCENTASHSFSK"

What was the orignal text?

5. When you are done with this, we will learn how to break Columnar Transposition.