Week 6 Friday

Make sure you're sitting next to someone!

Make sure you know your neighbors' names, and then discuss:

You have just intercepted a long piece of Vignère ciphertext. Based on an analysis of indices of coincidence, you think that the period is probably 5. When you rewrite the ciphertext into a rectangle of width 5, you find that the the most frequent letter in the third column is `F`.

Given just this information, come up with some words that *might* be the keyword that was used for encryption, and also some words that *probably aren't* the keyword.

Known-Plaintext Attack on Simple Substitution

1. Here is some ciphertext. Ignore the spaces; they are only there for visual convenience:

HRRH AHAQ HYVC HQBU XXUV POVX XQDC

This ciphertext was encrypted using simple substitution and the corresponding plaintext is known to contain the word TEETH. How many pattern matches for TEETH are there in this ciphertext?

(A) 1

(B) 2

(C) 3

(D) More than 3

2. Suppose that the plaintext frequencies of B, A, and N are 1.5%, 7.3%, and 7.4%, respectively. You intercept a 1000-letter ciphertext encrypted using simple substitution and known to contain the word BANANA. One of the pattern matches for BANANA that you find in your ciphertext is QUNUNU. Below are the observed counts of letters in the ciphertext. What is the value of G associated to QUNUNU?

A	B	C	D	E	F	G	H	I	J	K	L	M
64	1	64	64	15	77	66	2	1	27	22	10	27

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
15	46	18	83	126	32	7	93	0	20	26	24	70

Perfect Secrecy

3. What do you think were the salient points in the reading about perfect secrecy? Discuss with your neighbors and come up with at 1–3 things together.