Week 6 Tuesday

Make sure you know your neighbors' names. Then discuss:

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?

Known-Plaintext Attack on Simple Substitution

1. 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

Primes, Euler's Phi Function

2. Which of the following is largest?

(A) $\phi(13)$

(B) $\phi(20)$

(C) $\phi(24)$

(D) $\phi(30)$

3. How many primes p are there such that $29^p + 1$ is divisible by p?

4. The statement "$\phi(2n) = \phi(n)$" is true for...

(A) All positive integers n

(B) Some positive integers n

(C) No positive integers n