CMSC 389T HW4 SOLUTION

Phong Dinh and William Gasarch

Jan 10, 2017

Problem 5

Alice and Bob want to use a variant of Vigenere cipher where they code a sequence of affine ciphers rather than a sequence of shift cipher.
Part a: Alice and Bob first try to do this by having the key word be two keywords of the same length (like JUSTIN GRADES) and use the first one for the a needed for the affine cipher and the second one for b (RECALL that affine cipher maps x to $ax + b \pmod{36}$). Show that there are pair of words for which this is a bad idea. Give such a pair and explain why.

NOTE that we denote $A = 0$, $B = 1$, and so on.
An example: We use KEYWORD = CLYDE STAYS. Since $'C' = 2$, and 2 is not relatively prime with 36, then this is a bad approach to use affine cipher.
In general, as long as you give any example where $ax + b$ combination satisfies that a is not relatively prime with 36, then using affine cipher for Vignere is a bad idea.

Part b: Propose a way that Alice and Bob CAN easily have two words of the same length translated to a sequence of affine cipher.

We present a simple algorithm that works for any pair of same length words. First, notice that we will mostly focus on the first word, where the corresponding a has to be relatively prime with 36. Suppose that the the keyword is LARRY SWIMS, then for each letter in the first word, if its value is not relatively prime with 36, then we will increase its value (without changing the letter) until we reach the value that's actually relatively prime with 36.
In our case, LARRY = 11 0 17 17 24, then

$$11 \to 11$$
$$0 \to 1$$
$$17 \to 17$$
$$17 \to 17$$
$$24 \to 29$$

because 11, 1, 17, and 29 are all relatively prime to 36.

ANOTHER acceptable solution is adding a unique character (such as '!', or '?') to make the alphabetical letter now has 37 letters, then any pair of same length words should be a good keyword since 37 is a prime by itself.
If you limit your first word by restricting them be only the letter that are relatively prime with 36, you will not earn any credit.