QUESTION3

Since we are dealing with bigrams, 30*30= 900 is the modulus. The model of bigram is going to be { AA,AB,AC……. !!}. There are 900 options. However, for the key space alpha value should be smaller than 900 at the same time gcd of alpha and 900 should be 1. The phi of 900 is 240 which means there are 240 values that are smaller and relatively prime to 900.For the beta value the range is 0 to 899. Thus the key space is 240* 900 = 216.000 .

QUESTION4

Each bigrams point to a value 0 to 899. ({AA…….!!}). Then encoded number is found by multiplying first index with 30 and adding the value of second index.For each pair this value is unique. While encryption we are multiplying these encoded values with alpha and adding beta values on modulus 900. Since these values are fixed for a key the ciphertext bigrams that are pointing are also unique.

If an atacker knows that the plaintext is enrypted using bigrams, than he might end up with frequency bigrams and try to find the most frequent bigram and match it with the most frequent plaintext bigram on his table.

Thus, this affine cipher that is defined in question3 is not secure against the frequency letter analysis.

QUESTION6

Let us assume a letter of a plaintext and it's corresponding cipher letter. We do know that key is uniformly distributed and its probabilty P(k)= 1/29 for each letter. We have no idea of probability of plaintext being any letter, however total probability of each letter should sum up to 1.

Let us think about probability of having the letter 'C' in a ciphertext letter. If plaintext letter is A key should be C, if p.letter is B key should be B , if p.letter is C key is A ….. Notice that for each letter there is only unique value of key. And probability of each key values are 1/29.

Probability of plaintextletter X = P(Px) (Prob of p.letter A is P(Pa), B is P(Pb)

Prob of key that points to desired ciphertext = 1/29

Total = P(Pa) * 1/29 + P(Pb) * 1/29 + P(Pc) * 1/29 + …….. P(Pz)*1/29

Total includes every single chance for each plaintext letter corresponding to C.

Let's organize the total:

(P(Pa)+ P(Pb)+ P(Pc)+ P(Pd)+……P(Pz)) * 1/29 =

Notice that (P(Pa)+ P(Pb)+ P(Pc)+ P(Pd)+……P(Pz)) = 1

Total = 1 * 1/29 = 1/29 (Total is probabilty of ciphertext letter being 'C')

For every other ciphertext letter β, where β ∈ {A, B, C, Ç, …, Z} total is the same because of the above conditions.