Group-3

Mathematically compare the securities of additive and vignere cipher.

Answer:

The question has been asked about the securities of vignere cipher and additive cipher.
By security, we mean the number of attempts required to find the key and hence decipher the cipher text. The number of attempts is directly proportional to the number of possible keys combination. More combination causes more attempts to break. So, we're being asked about comparing number of possible keys combination in vignere and additive cipher.

Now, in additive cipher the number of possible keys combination can be 26 only because of the length of english alphabets. Starting from 1 to 26 , Eve can try each combination until he or she gets some meaningful plain text. Whereas, vignere cipher is multiplication of additive ciphers. By saying that we mean using a key of fixed length multiple times until it matches the length of plain text. So the number of possible keys combination is product of length of key and length of english alphabet combination. I.e. (key length)*26. In worse case, the key length will be equal to the length of plain text, hence we can write,
Total cost=(plain text length)* 26
This surely implies that vignere cipher is very much secured as compared to additive cipher, since number of keys combination in vignere is more than additive cipher.