# Project Continuation

Student Name: - Tolulope Olugbenga
Student Number: - 3643581
Course Number: - CS6355

## Questions/ Answers

1. The solutions has been uploaded with the other files.

2. Normally to break the Vigenere Cipher; it involves using the index of coincidence (to find the length of the key) and then using the Chi-Square statistics to find the key. Because, the length of the key is known, Chi-Square statistics. The process will involve deciphering the code with each of the 25 possible Caesar ciphers, and comparing the frequency distribution of the deciphered text with the frequency distribution of English alphabets for each key which generates 26 values for the Chi-squared statistic. The correct key will correspond to the deciphered text with the lowest Chi-squared statistic.

   The key identified by the programming code was 'MATH' which decoded the message to; "COMPUTERS - FROM MOBILE PHONES TO TABLETS TO LAPTOPS, DESKTOPS, SERVER AND MUCH MORE - TOUCH NEARLY EVERY ASPECT OF DAILY LIFE IN TODAY'S MODERN WORLD. TECHNOLOGY IS POWERED NOT JUST BY SILICON CHIPS AND ELECTRICITY, BUT BY THE CREATIVITY AND INGENUITY OF COMPUTER SCIENTISTS WHO TRANSLATE SOCIETY'S NEEDS AND WANTS INTO PRODUCTS THAT CAN IMPROVE BOTH SOCIETY AND THE ECONOMY."

3. Alice can apply a nonce to each file and encrypt such that $R = E(K, F||N)$, where $K$ is the key, $F$ is the file and $N$ is the nonce. N should be of considerable size to change the size of $R$, $S$, such that the $R$ will not be equal to any matching file that the cloud has. Alice should then create the hash of R such that $D = H(R)$ where D is the resulting hash and H is the hash function. Alice can then use D and S as indexes to search for the encrypted files she wants on the cloud.