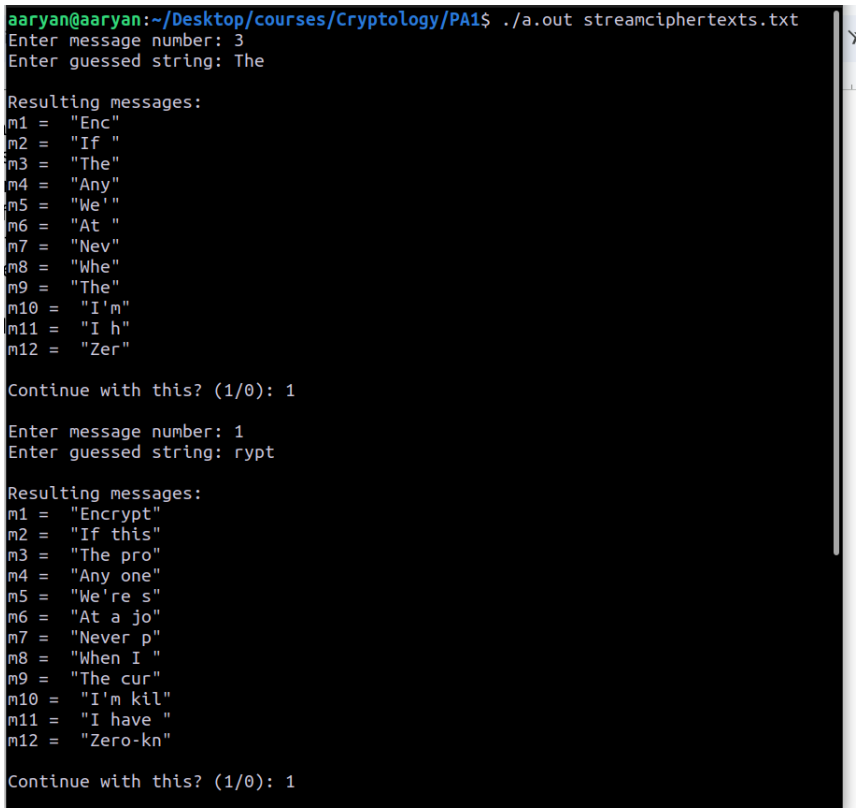
Programming Assignment 1
Aaryan, CO21BTECH11001

The program named “co21btech11001_src.cpp” is a C++ program which can be used to find the key and the messages using guess and validate method. You can enter a message number and a string, indicating that you are guessing that string as the part of the message. Then you can see the result of all the messages when you guessed that string. Then the program ask you if you want to continue with this or not. If yes, you will then guess the next part of the string. If not, then you will guess the same part again.

Here is a typical example:



Note: To run the program, first compile the code using “g++ co21btech11001_src.cpp”, then run the executable and provide the name of the ciphertext file in the command line, i.e. “./a.out streamciphertexts.txt”.

When decryption is completed, the program will output a file named “output.txt”, which contains all the messages and the key.

First message: “Encrypt, then MAC, is the correct order for secure authenticated encryption.”
Last message: “Zero-knowledge interactive proof: whatever you could compute before you interacted with me and afterward are not different. Shafi Goldwasser”

Key (in 8 bit integer format): [201, 185, 116, 95, 158, 226, 145, 176, 149, 23, 140, 204, 45, 231, 176, 101, 78, 215, 188, 24, 228, 178, 49, 91, 248, 85, 134, 201, 35, 112, 251, 76, 229, 99, 123, 46, 13, 86, 138, 24, 104, 182, 20, 140, 91, 108, 195, 20, 160, 77, 185, 122, 20, 0, 165, 8, 237, 6, 34, 249, 24, 138, 187, 84, 56, 47, 199, 70, 224, 68, 166, 33, 110, 77, 21, 163, 50, 65, 137, 8, 18, 96, 134, 73, 104, 0, 210, 70, 2, 225, 201, 51, 158, 3, 230, 202, 193, 244, 165, 107, 84, 65, 171, 12, 172, 55, 117, 98, 192, 56, 144, 179, 58, 133, 80, 79, 36, 20, 13, 15, 21, 120, 177, 58, 50, 178, 202, 10, 209, 72, 4, 68, 139, 203, 217, 247, 19, 242, 33, 35]