INTRODUCTION TO CRYPTOGRAPHY – PROJECT 2

B.Tech. Computer Science and Engineering (Cybersecurity)

|  |  |
| --- | --- |
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of submission: 12/12/2021 |

**Code:**

Language: C

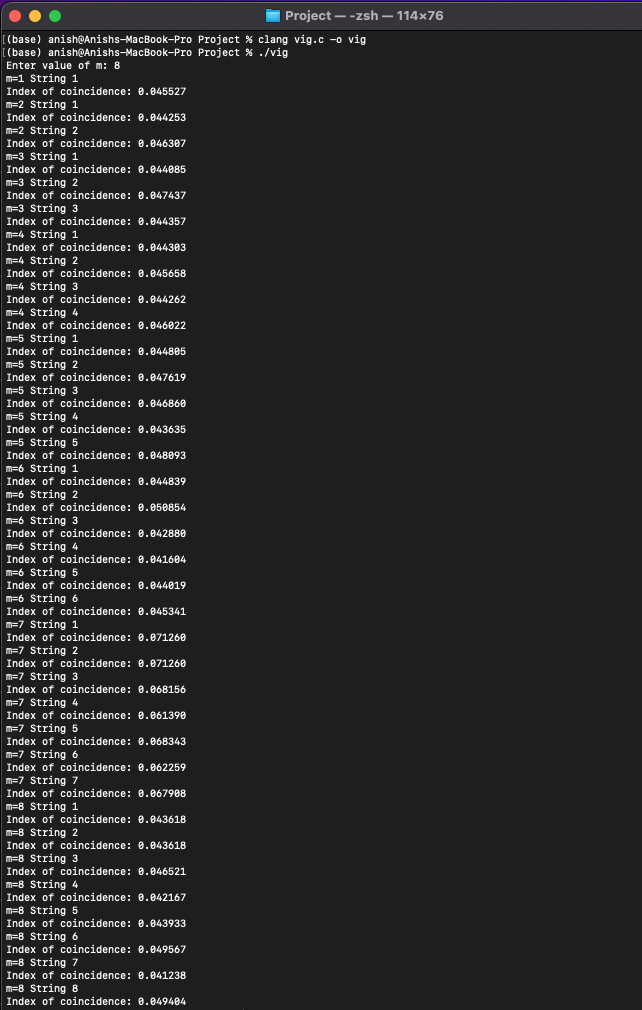
Editor: Atom

Compiler: clang/ZSH

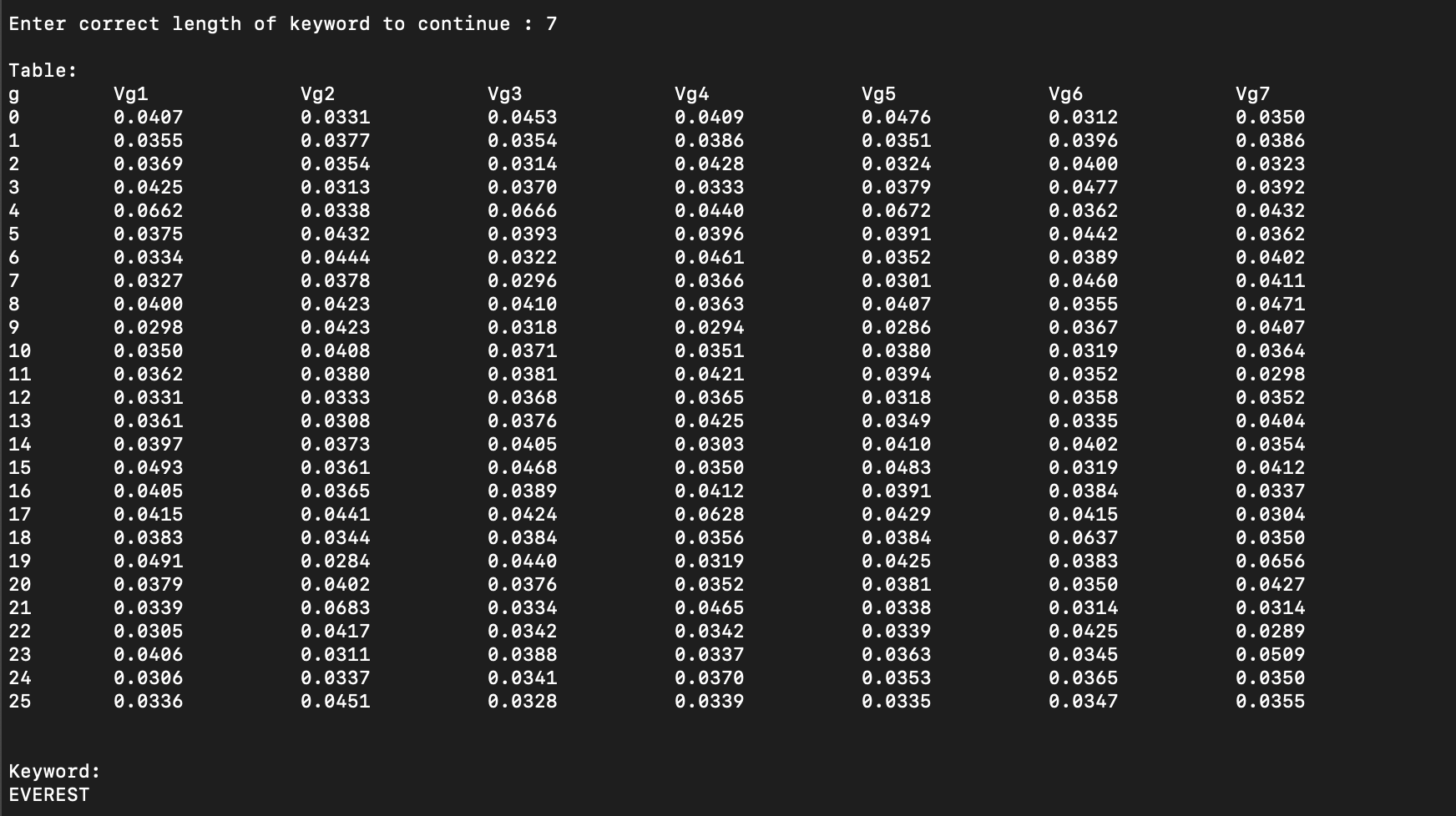
Part 1: Verification of keyword length assumption through Index of Coincidences method

IMAGE ON NEXT PAGE

Via the diagram we can confirm that the Indices of the strings of m=7 are much closer to 0.065 than those of any other string.

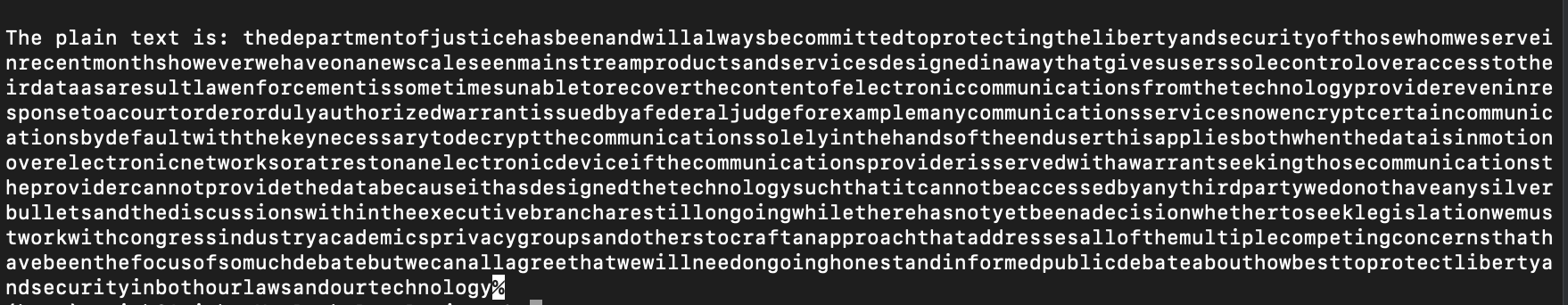


Part 2:



Keyword: Everest

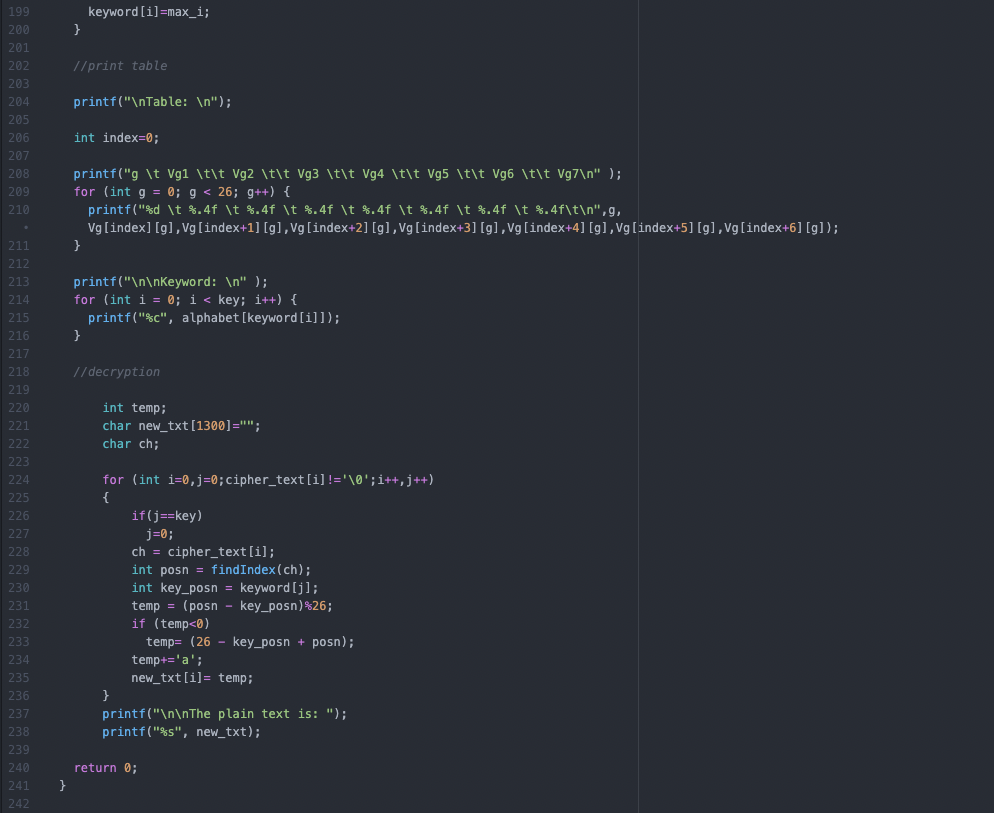
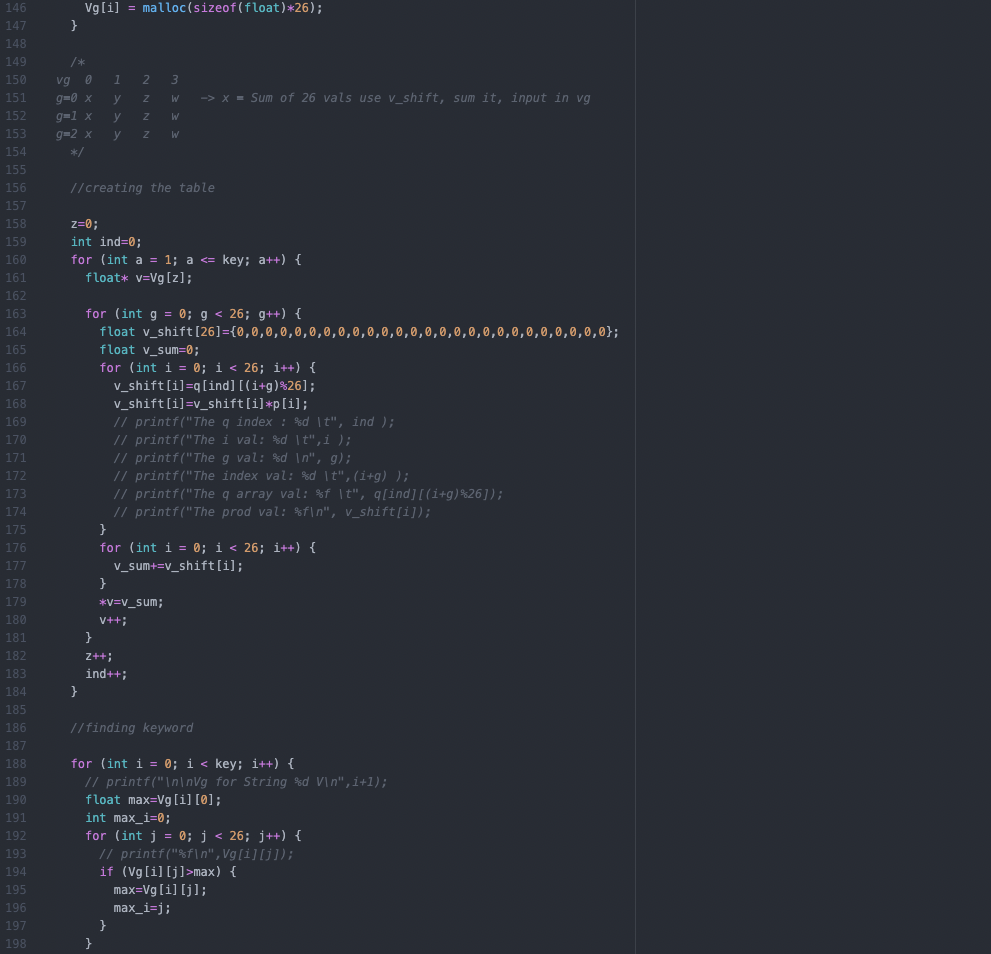
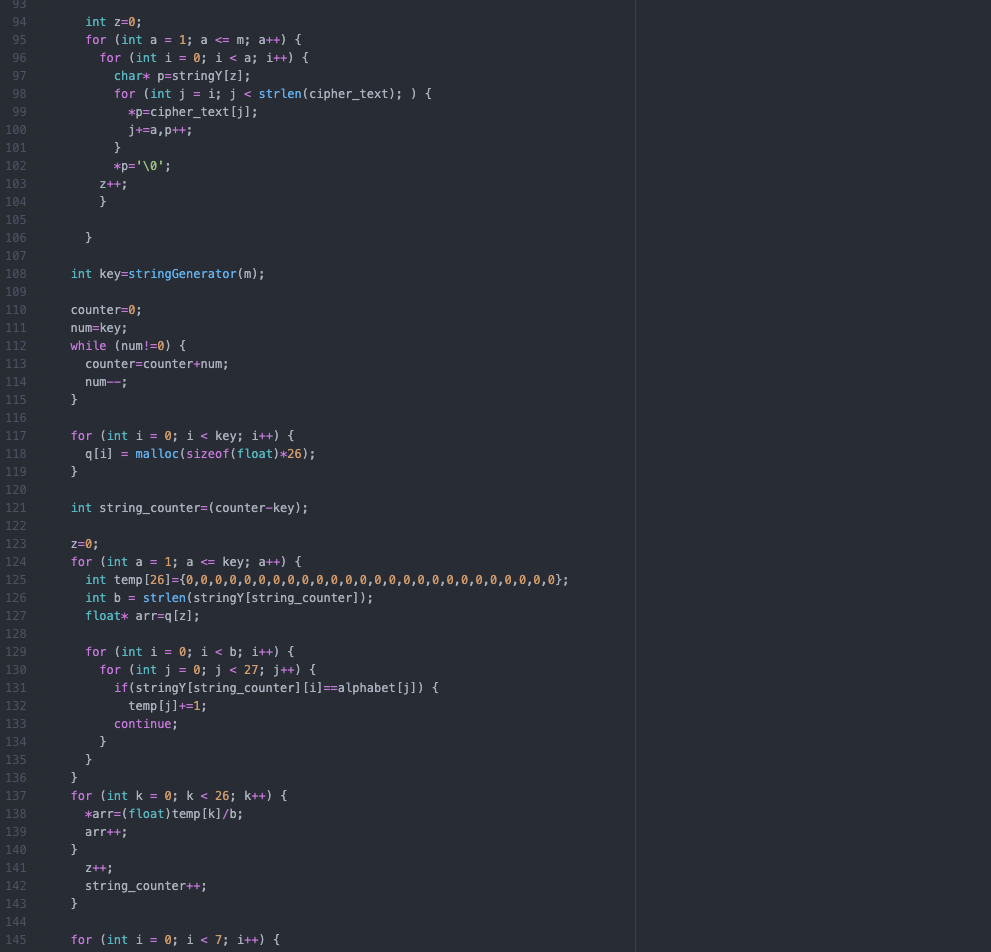
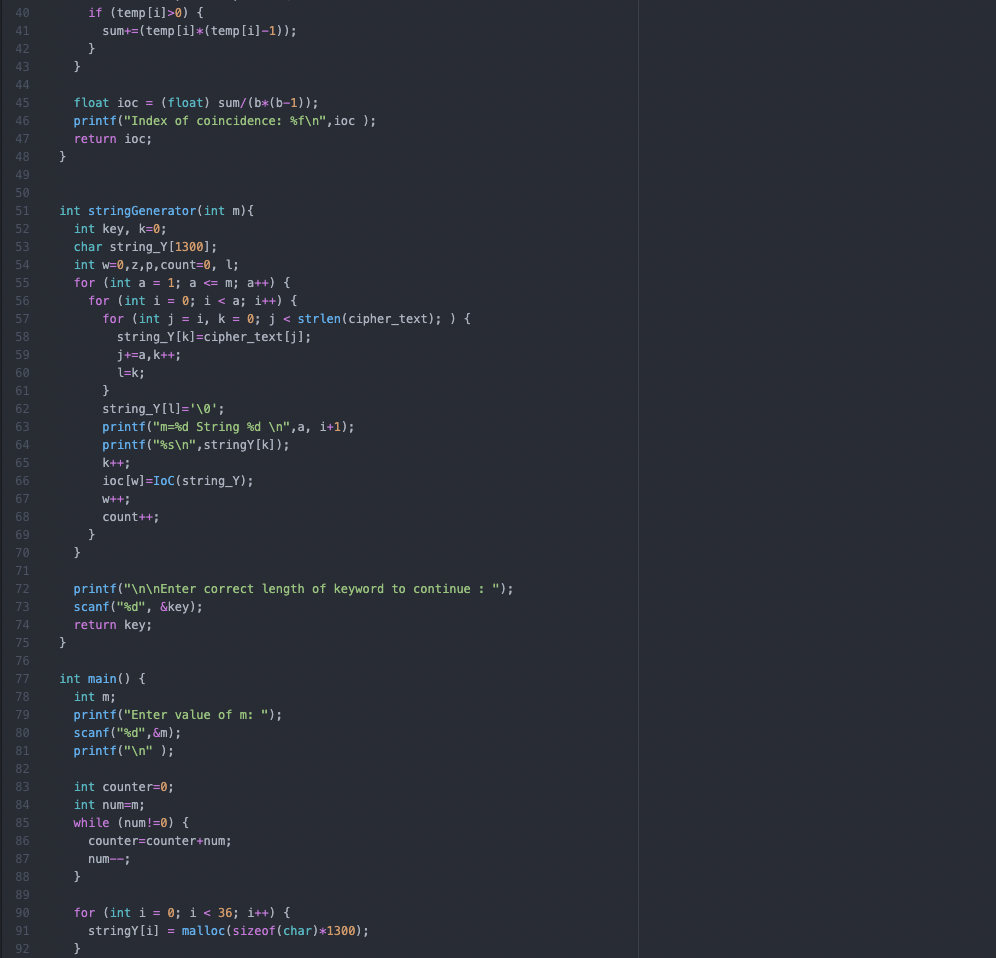
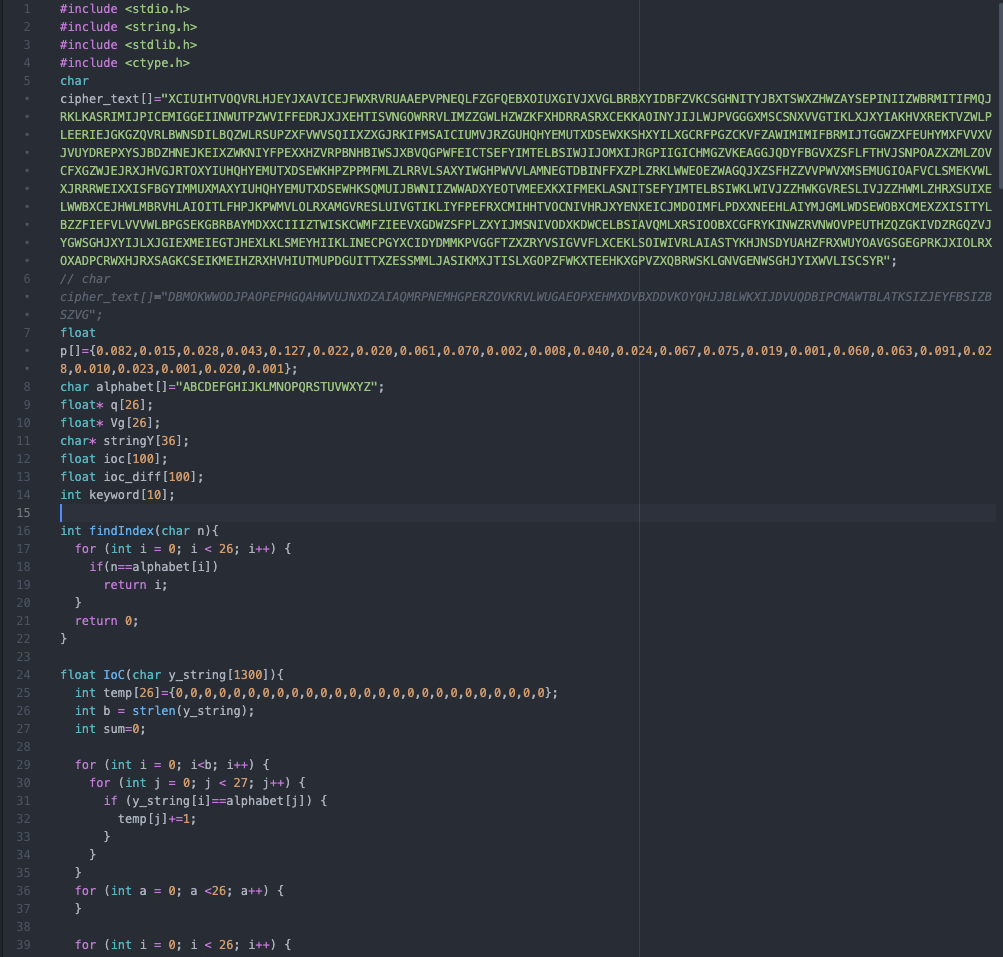
Part 3: Plaintext



Formatted Plaintext:

The department of justice has been and will always be committed to protecting the liberty and security of those whom we serve. In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly authorized warrant issued by a federal judge. For example, many communications services now encrypt certain communications by default, with the key necessary to decrypt the communications solely in the hands of the end user. This applies both when the data is in motion over electronic networks, or at rest on an electronic device. If the communications provider is served with a warrant seeking those communications, the provider cannot provide the data because it has designed the technology such that it cannot be accessed by any third party. We do not have any silver bullets and the discussions within the executive branch are still ongoing. While there has not yet been a decision whether to seek legislation, we must work with congress, industry, academics, privacy groups and others to craft an approach that addresses all of the multiple, competing concerns that have been the focus of so much debate. But we can all agree that we will need ongoing honest and informed public debate about how best to protect liberty and security in both our laws and our technology.

**Code:**

****

**Complete Output:**

