Amina Haq, David Wilson, Jean Pauline Arcita

CEG 4710, Spring 2021

Project 03 Report

# Introduction

Our goal for this project was to develop a program that could perform a brute force attack to break the encryption on a set of provided files encoded with AES. We were provided the last 96 bits of the 128-bit key, so our program only had to find the first 16. We selected our test files based on a modulus operation on one of our member’s University ID (UID) numbers. The rest of this report will describe the input to this task, the work itself, and the results.

# The Input

We chose to use the UID number belonging group member David Wilson. To determine which test files we should use for the program, we took the last four digits of David’s UID as an integer: 3925. We then performed a modulus operation on this integer and its reverse-ordered sibling, 5293. The results are shown in Equations 1 and 2.

|  |  |
| --- | --- |
|  | (1) |
|  | (2) |

As a result, we chose to use test files 02.e and 12.e in our program.

# The Work and the Results

Our program was designed to iterate through all possible combinations of the 16-bit subkey from “aaaa” to “zzzz.” Each time it did this, it would scan through the output to determine the percentage of the results that could be interpreted as standard alphanumeric English characters or basic punctuation. When this percentage reached at least 90%, we would stop and print the output. The results of these operations are shown in Figures 1 and 2.

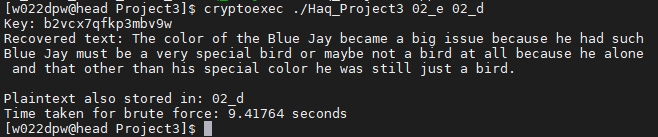


Figure : Decryption of the test file 02.e

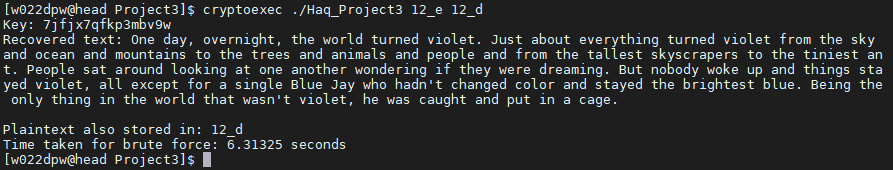


Figure : Decryption of the test file 12.e

As the figures show, both files were fully decoded into proper English. The sub-key for 02.e turned out to be **b2vc**, while the sub-key for 12.e turned out to be **7jfj**. We also completed the bonus object by calculating the elapsed time it took to find these keys via the brute force method. For convenience, these values will be recounted in Table 1.

Table : Complete statistics for test file decoding

|  |  |  |
| --- | --- | --- |
| **Test File** | **Key** | **Elapsed Time** |
| 02.e | b2vcx7qfkp3mbv9w | 9.41764 seconds |
| 12.e | 7jfjx7qfkp3mbv9w | 6.31325 seconds |