Encryption Virtual Machines-Computer Science Project

By: Abhilash Balaji and Mayank Baranwal

Name of Project: Encrypting Virtual Machines

Description of Project & Methodology

Traditional ciphers such as the Caesar or Atbash ciphers had a major problem of having a constant relationship between the unencrypted and encrypted letters, i.e. one letter would be constantly encrypted to another letter. As such, these ciphers could be easily cracked as they could be subject to frequency analysis as some letters appeared more often than others

This encryption program will not be susceptible to the above mentioned strategy. In our program, the unencrypted message is passed through a series of letter relationships which keep incrementing in the order of hundreds, tens and ones. Shown below is an example with only 6 letters,” a, b, c, d, e and f.” (Orginal Message: FADE)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | D |  | D | C |  | C | F |  | F |
| B | F |  | F | E |  | E | E |  | E |
| C | A |  | A | D |  | D | C |  | C |
| D | B |  | B | F |  | F | B |  | B |
| E | C |  | C | A |  | A | D |  | D |
| F | E |  | E | B |  | B | A |  | A |
| Incremented Every Letter | |  | Incremented After 10 Letters | |  | Incremented After 100 Letter | |  | Reflector |

It is seen that the letter “F” becomes “C.” After this, the first rotor has incremented its rotors once so the next letter doesn’t follow the same letter relationship. It is also interesting to note that if “C” is inputted into the system, we get back “F.” This allows for effective decryption of the code.

Sample Output:

User inputs string “TEST PHRASE” which gets encrypted to “SBFB VUOGWQ.” When this encrypted string is re-inputted into the machine with the same starting configuration, we obtain the original string, “TEST PHRASE.”