Project 2

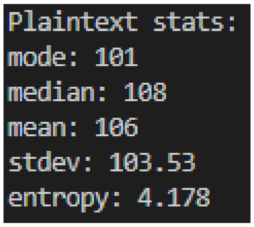
CECS 564

Spring 2020

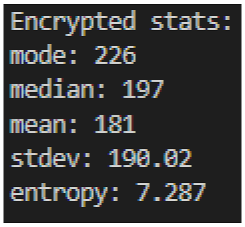
Roman Millem

The Content Scrambling System (CSS) was implementing in the c++ language on a windows 10 OS using the visual studio code IDE. My application begins by initializing LFSR1 using the first 3 bytes of the key and LFSR2 using the last 2 bytes. Then the 4th bit of each register is set to 1 to prevent the 0 state. Then, for each character, a keystream is created by executing 8 shifts in both of the registers, harvesting the 8 most significant bits of each register, then adding them using a full adder system with the initial carry bit set to 0. So, for the first byte, 8 shifts are made, followed by 16 shifts for the 2nd, 24 for the 3rd, and so on. The system resets after each byte is calculated meaning the first 8 shifts are the same for each byte following the first and so on. This is not a very cost efficient method, so the given "text data" text file was used instead of the "Darwin.txt" as using the Darwin text file would take too long to run.

Using the given "text data" text file, the summary statistics were calculated and are shown below:



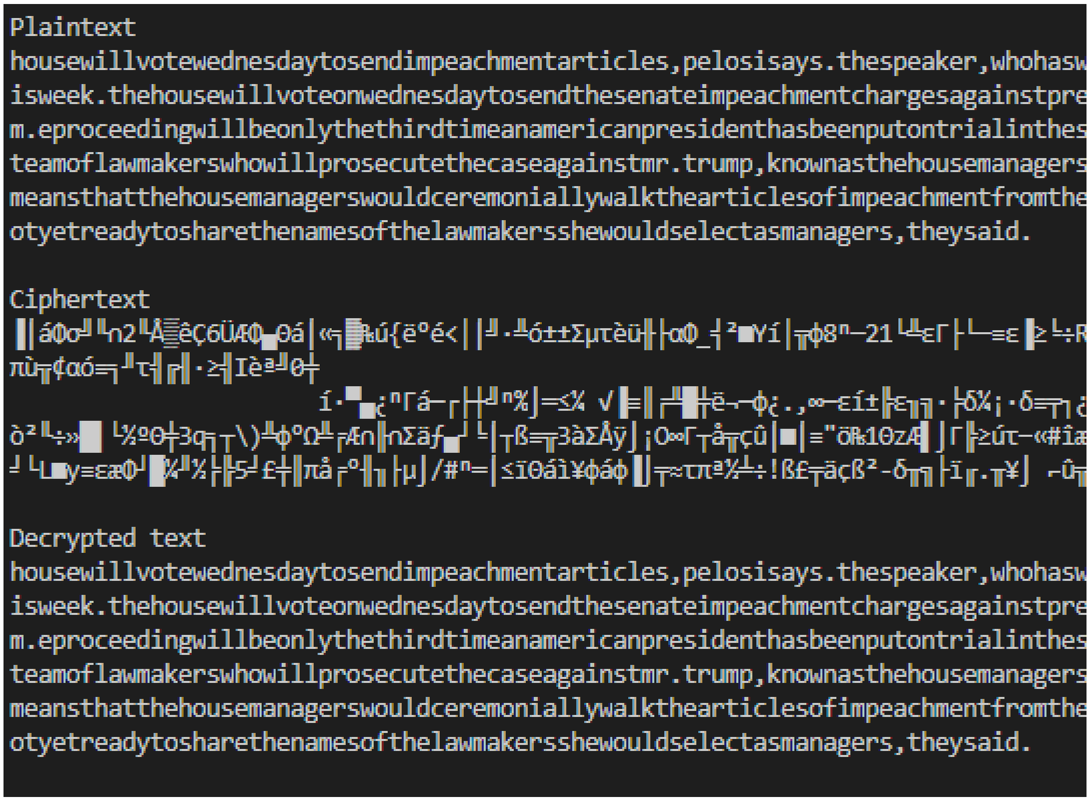
```
Plaintext stats:
mode: 101
median: 108
mean: 106
stdev: 103.53
entropy: 4.178
```



```
Encrypted stats:
mode: 226
median: 197
mean: 181
stdev: 190.02
entropy: 7.287
```

The security of the system is significantly increased as the entropy of the ciphertext is nearly 60% higher than the entropy of the plaintext. Most characters in the ciphertext are extended ASCII characters, which is concurrent with the resulting mean, median, and mode. However there some resulting encrypted characters result in lower values. This causes a strange output. For example, a resulting value of 13 with translate to a carriage return and the output will print over itself beginning at the start of the current line. This was handled for decryption purposed by storing the integer value in an array so that each character can be translated individually.

The encryption and decryption of the “text data.txt” file is shown below:



```
Plaintext
housewillvotewednesdaytosendimpeachmentarticles,pelosisays.thespeaker,whohasw
isweek.thehousewillvoteonwednesdaytosendthesenateimpeachmentchargesagainstpre
m.eproceedingwillbeonlythethirdtimeanamericanpresidenthasbeenputontrialinthes
teamoflawmakerswhowillprosecutethecaseagainstmr.trump,knownasthehousemanagers
meansthatthehousemanagerswouldceremoniallywalkthearticlesofimpeachmentfromthe
otyetreadytosharethenamesofthelawmakersshewouldselectasmanagers,theysaid.

Ciphertext
▐║áΦσ╜╙n2╙Å▒êÇ6ÜÆΦ▄Θá│«¬▒ßú{ë°é<││╛·╨ó±±Σµτèü╫├αΦ_╡²■Yí│╥φ8ⁿ─21╙╧εΓ├└─≡ε▐≥╘÷R
πù╥¢αó╤┐╜τ╣│╓║·≥╡│Iè╛╝Θ╪
                                 í·▀▄¿ⁿΓá─┌├╫╛ⁿ%⌡═≤¼ √▐≡║┌╨█╫ë¬─φ¿.,∞─εí±╟ε╖╖·├δ%¡·δ╤┐¿
ò²╙÷»█ ╘½º0╪3q┐┬\)╩φ°Ω╧╤Æn║nΣäƒ▄┘ ╘│┬ß═╤3àΣÅÿ⌡¡O∞Γ┬å╤çû│■│≡"öR1ΘzÆ▌⌡Γ╟≥úτ─«#îæ
╛ └L■y≡εæΦ╜▐¼╜½├╟5┘£╪║πå╒°╢╖├µ⌡/#ⁿ═│≤ïΘâì¥φáφ▐║╤≈τπª½┴÷!ß£╤ãçß²-δ╖╕├ï╓.╥¥⌡ ⌐û╥

Decrypted text
housewillvotewednesdaytosendimpeachmentarticles,pelosisays.thespeaker,whohasw
isweek.thehousewillvoteonwednesdaytosendthesenateimpeachmentchargesagainstpre
m.eproceedingwillbeonlythethirdtimeanamericanpresidenthasbeenputontrialinthes
teamoflawmakerswhowillprosecutethecaseagainstmr.trump,knownasthehousemanagers
meansthatthehousemanagerswouldceremoniallywalkthearticlesofimpeachmentfromthe
otyetreadytosharethenamesofthelawmakersshewouldselectasmanagers,theysaid.
```

The text is partially cut to make the screenshot viewable.