7402 Asn 5 Design

“Filled to the brim with Confusion”

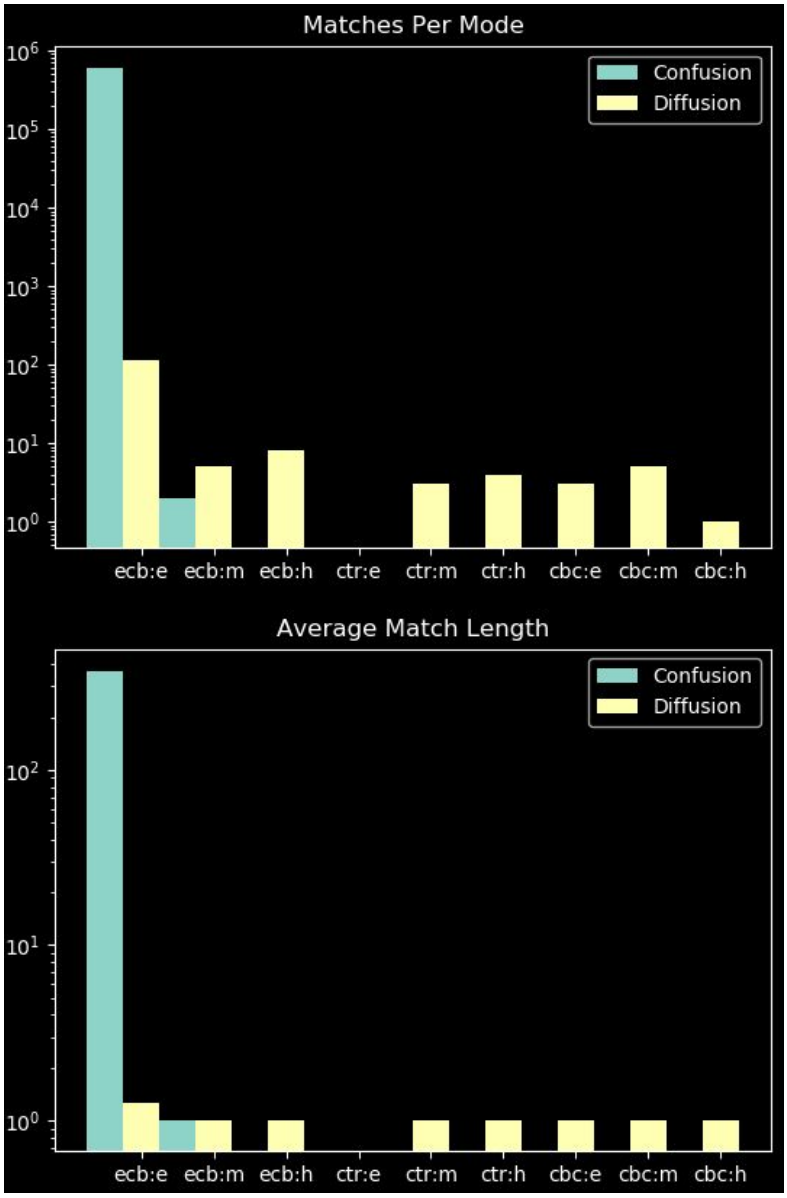
Isaac Morneau; A00958405
John Agapeyev; A00928238

Bonus

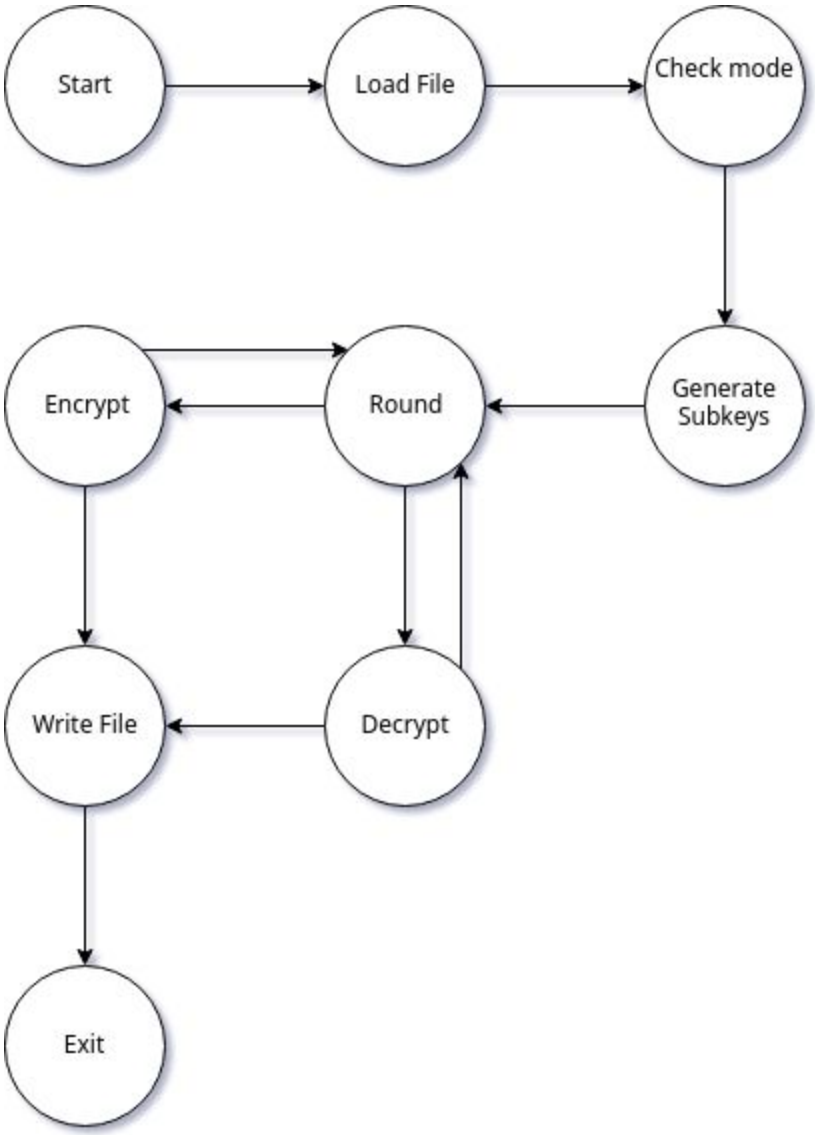
The noteworthy additional features are:

Graphing of automated analysis of diffusion and confusion

AES for the hard mode as a method of our comparison for medium mode which was an amuature attempt. Easy mode was intentionally created to be poor.



FSM


Start
Load File
Check mode
Encrypt
Round
Generate Subkeys
Write File
Decrypt
Exit

Pseudocode

Start

Allocate buffers
Goto Load File

Load File

Load the bytes of the file into memory
Ensure the data is the right size
Goto Check Mode

Check Mode

If mode is cbc or ctr
    generate iv
Goto Generate Subkeys

Generate Subkeys

For each round generate a subkey.
Goto round

Round

Select the round key

If mode is encrypt
    Goto Encrypt
Otherwise
    Goto Decrypt

Encrypt

Run the feistel function forward (encrypting) over the data
If there are more rounds
    Goto rounds
Otherwise
    Goto Write File

Decrypt

Run the feistel function inverted (decrypting) over the data
If there are more rounds
    Goto rounds
Otherwise
    Goto Write File

Write File

Write the modified data to the output file
Goto End

End

Free resources