DES - Security Through Obscurity

Monica Singh, Matt Frederick, George Wood, Brandon Crane

30 September 2017

1 Individual Contributions

Team members did most of the work together. Pair programming was implemented in the beginning to code individual modules. Matt and Monica worked together in one pair, and George and Brandon in another. These modules were then placed in the main file accordingly. Once debugging started, it became a whole team effort with everybody analyzing the output. To verify that our encryption was working correctly, George took it upon himself to run through the algorithm by hand. He worked with a very simple key and plaintext. This process was compared to the output of the bit strings that our program output before and after steps in the algorithm. This processes verified that our encryption was accurate, and we were able to continue debugging to completion as a team. Brandon drafted up the latex document, and George created the graphs.

2 Time Graphs for 8 Rounds

8 Characters (64 bits)

Encryption:

Decryption:

8000 Characters (64000 bits)

Encryption:

Decryption:

80000 Characters (640000 bits)

Encryption:

Decryption:

3 Time Graphs for 16 Rounds

8 Characters (64 bits)

Encryption:

Decryption:

8000 Characters (64000 bits)

Encryption:

Decryption:

80000 Characters (640000 bits)

Encryption:

Decryption:

4 Code (C++)