Requirements

# Functional Requirements

1. The system shall implement cryptographic algorithms with NIST standards.
2. The system shall receive input from the console with specific commands.
3. The system shall accept a “-ex” tag/modifier for a detailed explanation on the algorithm.
4. The system shall not use external libraries.
5. The system shall be able to print out a detailed description of each algorithm
6. The system shall show a cryptanalysis method for each algorithm if one exists.

# Non-functional Requirements

1. The system shall be a console application
2. The system shall be written in Python
3. The system shall be designed to incorporate a GUI in a future update.
4. The system shall be executed in a local environment.

# Domain Requirements

1. The system shall implement a Caesar Cipher
2. The system shall implement a Vigenère Cipher
3. The system shall implement a Rail fence Cipher
4. The system shall implement a Hill Cipher
5. The system shall implement DES
6. The system shall implement AES
7. The system shall implement RSA
8. The system shall implement Diffie-Hellman
9. The system shall implement ECC
10. The system shall show ECB
11. The system shall show CBC
12. The system shall show CFB
13. The system shall show OFB
14. The system shall show CTR
15. The system shall show GCM