Division of Labor Statement

Kelvin Chen:

- **Section:** 4.1 MD5 Collisions
- **Word Problems:** Questions 1 & 3
- **Responsibilities:**
  - Documented the MD5 collision process using tools like Evilize and Selfextract.
  - Described the tool setup, collision generation, and attack implications.
  - Addressed mitigation strategies for MD5 collision vulnerabilities in the word problems.
  - Provided detailed steps for generating executable collisions and how they impact file integrity.

Cara Dong:

- **Section:** 4.2 SHA-1 Collisions
- **Word Problems:** Questions 1 & 2
- **Responsibilities:**
  - Explored SHA-1 collisions using both online and offline tools, referencing the SHAttered attack methodology.
  - Documented the methods for generating SHA-1 collisions with PDF and image files.
  - Discussed the implications of SHA-1 vulnerabilities on TLS security.
  - Provided in-depth analysis of how the gained knowledge from factorable moduli can be used in TLS attacks.

Kang Karwai:

- **Section:** 4.3 Certificate Generation
- **Word Problems:** Question 5
- **Responsibilities:**
  - Worked on generating RSA certificates of varying sizes, modifying OpenSSL source code to bypass minimum key length restrictions.
  - Documented the certificate creation process, including key generation, modulus extraction, and public key generation.
  - Identified and described challenges encountered during certificate generation and key extraction.
  - Analyzed requirements for decrypting TLS sessions using Diffie-Hellman and Elliptic Curve key exchanges.

David Xiao:

- **Section:** 4.4 Factoring & Decryption
- **Word Problems:** Question 4
- **Additional Responsibility:** Final Report Integration
- **Responsibilities:**
  - Focused on factoring RSA moduli and decrypting TLS sessions using the obtained factors.
  - Experimented with various factoring tools such as MSIEVE and CADO-NFS, documenting tool setup, resource usage, and limitations.
  - Provided a comprehensive breakdown of the decryption process after modulus factorization.
  - Estimated factoring capabilities based on available hardware resources.
  - Consolidated all group members’ contributions into the final cohesive report, ensuring consistency, formatting, and clarity across sections.