1. Discussion board
    i. Why symmetric key cryptography alone cannot resolve Internet security issue?
    ii. Why is it important to study the Feistel cipher?
    iii. List ways in which symmetric keys can be distributed to two communicating parties.
    iv. Which of the following security services are provided by using symmetric key to encrypt and decrypt messages
        - Authentication
        - Confidentiality
        - Integrity
    v. What is the key size for Caesar cipher whose legimate characters are

        ```
        abcdefghijklmnopqrstuvwxyz
        ```

    vi. What is the key size for Caesar cipher whose legimate characters are

        ```
        abcdefghijklmnopqrstuvwxyz1234567890
        ```

2. If the key of a Transposition Ciphers is **MATRIX**, what is the ciphertext for the plaintext

    ```
    bruceleeisareallycoolguy
    ```

3. Review Questions

    a. What are the essential ingredients of a symmetric cipher?
    b. What are the two basic functions used in encryption algorithms?
    c. How many keys are required for two people to communicate via a symmetric cipher?
    d. What is the difference between a block cipher and a stream cipher?
    e. What are the two general approaches to attacking a cipher?
    f. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?
    g. What is triple encryption?
    h. Why is the middle portion of 3DES a decryption rather than an encryption?
    i. What is the difference between link and end-to-end encryption?

j. List ways in which secret keys can be distributed to two communicating parties.
k. What is the difference between a session key and a master key?
l. What is a key distribution center?

4. Please use Feistel cipher to manually encrypt and decrypt the plaintext **BRUCELEE**.
Note: The cipher has these parameters:

- Two rounds
- Function F() is a Caesar Cipher. Instead of using only 26 characters, the characters used in the Caesar Cipher are all the characters defined in an ASCII Table. Thus, if a character **NUL** in a plaintext will be encrypted as the character **STX** in a ciphertext if the key is 2.
- K1 is 2
- K2 is 3