Project 2: Design and Security Evaluation of a Simple Product Cipher

Objective:

Each group will design a custom product cipher that combines substitution and transposition techniques to enhance encryption security. The designed cipher will then be evaluated using two fundamental cryptographic metrics:

1. Strict Avalanche Criterion (SAC): Measures how significantly the ciphertext changes when a single bit in the plaintext or key is flipped. A strong cipher should produce a 50% change in the ciphertext on average.
2. Bit Independence Criterion (BIC): Examines whether changes in one bit of the input affect unrelated bits in the output, ensuring that individual bit modifications do not follow a predictable pattern.

Task Requirements:

1. Cipher Design:
   - Construct a block cipher that operates on 16-bit blocks of plaintext.
   - Implement a product cipher by combining a substitution layer (confusion) and a transposition layer (diffusion) to enhance security. You can use multiple rounds.
   - Your cipher should aim to closely satisfy the SAC and BIC properties for strong encryption.
2. Implementation:
   - Develop the cipher in Python, Java, or C++.
   - Implement both encryption and decryption functions to verify correctness.
   - Conduct security tests to measure SAC and BIC properties.
3. Report Submission (1-2 pages):
   - Cipher Description: Justify your choice of substitution and transposition techniques.
   - Implementation Details: Describe the encryption logic and programming language used.
   - Security Testing Results: Present SAC and BIC analysis results in a tabular format.

- Conclusion: Reflect on your cipher's performance and suggest improvements.

Grading Criteria (Total: 50 Points):

- Cipher Design & Explanation (10 points): Clarity and justification of the encryption approach.
- Working Implementation (15 points): Functional encryption and decryption with accurate execution.
- SAC and BIC Analysis (10 points): Quality of security evaluation and accuracy of results.
- Short Report (10 points): Well-structured documentation of the cipher and its security.
- Teamwork & Participation (5 points): Contribution and collaboration within the group.

Additional Requirements for CSCE-863 Students:

1. **Extended Block Size and Key Expansion**
   - Graduate groups must implement a **32-bit block cipher** instead of a 16-bit one.
   - They should **design and justify a key expansion mechanism**, ensuring that each encryption round uses a different subkey.
2. **Multiple Rounds of Encryption**
   - Graduate students must implement **at least 3 rounds** of their product cipher to enhance security.
   - The impact of increasing rounds should be analyzed with respect to **SAC and BIC properties**.
3. **Cryptanalysis Attempt**
   - Perform a **basic cryptanalysis** on your own cipher.
   - Attempt to break your encryption using **frequency analysis, differential analysis, or chosen plaintext attacks** and discuss the results.
4. **Extended Report (1-3 Pages)**

  - Include all standard sections from the undergraduate version.
  - Add a section analyzing the impact of **multiple rounds on SAC and BIC**.
  - Discuss the results of your **cryptanalysis attempt** and **comparative study** with standard ciphers.

Graduate Student Grading Criteria (Total: 70 Points):

- **Cipher Design & Explanation (15 points)**
- **Working Implementation (15 points)**
- **SAC and BIC Analysis (15 points)**
- **Cryptanalysis and Security Discussion (15 points)**
- **Extended Report (10 points)**