Topic 1. Cryptanalysis on Symmetric Ciphers

Scenario:

A cybersecurity firm wants to assess the strength of a newly developed symmetric cipher. They aim to identify potential vulnerabilities and weaknesses in the encryption algorithm.

Gaps, Motivations, and Desired Security Features:

- **Gaps**: Many symmetric ciphers, while theoretically sound, may have practical vulnerabilities when implemented.
- **Motivations**: To ensure that the symmetric cipher can withstand real-world attacks and is suitable for securing sensitive data.
- **Desired Security Features**:
  - Resistance to known plaintext attacks
  - Resistance to chosen plaintext attacks
  - Resistance to differential cryptanalysis
  - Resistance to linear cryptanalysis

Proposed Solutions:

- **Solution Architecture**:
  - **Ciphertext Collection**: Gather a significant amount of encrypted data for analysis.
  - **Cryptanalysis Tools**: Utilize specialized software to analyze the ciphertext.
  - **Attack Models**: Define specific attack scenarios to test the cipher's resistance.
- **Solution Details**:
  - **Data Collection**: Use the cipher to encrypt known data sets.
  - **Analysis**: Apply various cryptanalysis techniques to attempt to decipher the collected data without the key.

Implementation and Testing:

- **Implementation**:
  - Set up a controlled environment for encryption and data collection.
  - Implement the cipher and generate a significant amount of ciphertext.
- **Testing**:
  - **Functional Testing**: Ensure the cipher encrypts and decrypts correctly.
  - **Security Testing**: Use tools or your test case to attempt to break the encryption.
  - **Attack Scenarios**: Test against known plaintext, chosen plaintext, differential cryptanalysis, and linear attacks.

Deployment:

- If the cipher is found to be secure, it can be recommended for deployment in real-world applications.
- If vulnerabilities are found, they should be documented and shared with the cipher's developers for rectification.