Assignment 1: Quantifying Confusion and Diffusion

Course: CS6201E - Foundations of Information Security

Objective

This assignment aims to help you understand Shannon's principles of **confusion** and **diffusion** in cryptographic systems. You will attempt to propose measures that can quantify these properties for selected classical ciphers.
Max. Marks: 5
Submission Deadline: 24th September 2025

Tasks

Part A: Classical Ciphers

Consider the following ciphers discussed in class

- Shift Cipher
- Substitution Cipher
- Vigenère Cipher
- Hill Cipher
- Transposition Cipher
- ADFGVX cipher

For each chosen cipher, perform the following experiments:

(a) **Diffusion: Avalanche Effect** Encrypt a fixed plaintext. Make an incremental change in the plaintext and re-encrypt. Measure the fraction of ciphertext symbols that change. Repeat for multiple positions (and multiple plaintexts) and average the results.

(b) **Confusion: Key Sensitivity** Encrypt a fixed plaintext with a given key. Make an incremental change in the key and re-encrypt. Measure the change in ciphertext. Report average changes.

(c) **Statistical Measures** The end goal of this assignment is to propose metrics that can be used to quantify confusion and diffusion in classical ciphers. For this, you need to go through existing literature and understand the metrics commonly used to measure these quantities in modern ciphers. Given the differences in the input and output alphabets in classical ciphers and modern block ciphers, it is evident

that the same metrics cannot be used. What needs to be changed? What else needs to be considered when defining these metrics? Why? Once you define your measure, quantify confusion and diffusion for each of the ciphers mentioned above using your new metrics. Are your metrics better in explaining the phenomena? Why?

Applicability in the Modern World

Format Preserving Encryption (FPE) requires that the encrypted message retain the properties of the original message. For example, a sequence os 10 digits should still be encrypted as a sequence of 10 digits. In this domain, your new metrics will be helpful in quantifying confusion and diffusion.

Deliverables

- A research paper (4–6 pages) in IEEE format containing:
  - Introduction
  - Literature Survey
  - Methodology and experimental setup.
  - Tables/graphs (where required).
  - Comparative discussion: classical vs FPE.
- Well-documented source code (submit separately).
- You will be asked to give a 10 minute presentation in front of your class explaining your proposed metric, and the rationale for selecting that metric