Advancing Data Security with Iterative Encryption and Decryption using Adversarial Generative Networks for Enhancing Data Confidentiality and Integrity

1. Executive Summary:

This project proposes an advanced cryptographic framework that integrates iterative encryption, iterative decryption, and Adversarial Generative Networks (GANs) to overcome the limitations of traditional encryption techniques. With increasing cyber threats, existing static ciphers struggle to ensure confidentiality and consistency during attacks. The proposed adversarial-GAN-enhanced system

aims to dynamically strengthen encryption, improve tamper resistance, and enable intelligent decryption even in noisy or manipulated environments. This research focuses on enhancing data confidentiality and integrity across communication systems, secure storage, and high-risk data processing environments.

2. Problem Statement:

Traditional encryption mechanisms follow deterministic patterns that adversaries can learn and exploit. As data volumes increase and cyberattacks grow more sophisticated, classical encryption struggles against pattern recognition, key-guessing, and ciphertext manipulation. Moreover, static decryption systems often fail when data is partially corrupted or intercepted. There is a critical need for a dynamic, intelligent system capable of reinforcing encryption as threats evolve.

Objective:

• Develop an iterative encryption engine capable of multiple transformation layers.

• Use adversarial generative networks to simulate attacks and refine the encryption scheme.

• Train a discriminator-style decryption network that improves in accuracy during adversarial training.

• Ensure data confidentiality, tamper detection, and reliability during recovery.

3. Data Sources:

• Synthetic plaintext corpora generated through NLTK or curated datasets.

• Ciphertext generated from iterative multi-layer encryption pipelines.

• GAN-generated adversarial samples simulating manipulation and attack patterns.

• Supplementary text datasets for training robust decryption networks.

4. Methodology:

• Construct an iterative encryption system with multi-level character transformations.

• Implement a GAN framework where the generator creates adversarial ciphertext variants and the discriminator

(decryption model) learns to reverse transformations accurately.

• Create training loops integrating GAN cycles, perturbation-based attacks, and corrective learning.

• Evaluate encryption strength using entropy, diffusion-confusion metrics, and resistance to statistical attacks.

• Assess decryption reliability using recovery accuracy across adversarial noise and multi-layer transformations.

5. Expected Outcomes:

• A robust encryption architecture capable of resisting dynamic and adversarial attacks.

• A machine-learning-driven decryption engine with self-improving capabilities.

• Higher complexity ciphertext ensuring improved confidentiality.

• Reliable message recovery even under distortion, manipulation, or partial corruption.

• Practical applicability for secure communication, defense systems, and critical infrastructures.

6. Risks and Challenges:

• High computational cost due to iterative encryption cycles and GAN training.

• Difficulty in maintaining model stability between generator and discriminator.

• Risk of mode collapse in GAN training, reducing effectiveness of adversarial learning.

• Increased model complexity may slow down real-time communication systems.

7. Conclusion:

This project advances modern cryptography by integrating iterative encryption with adversarial machine learning. The proposed GAN-driven encryption-decryption pipeline enhances confidentiality, strengthens integrity validation, and increases resilience against evolving cyber threats. The resulting system provides a forward-looking, intelligent cryptographic model suitable for next-generation secure communication and data protection applications.