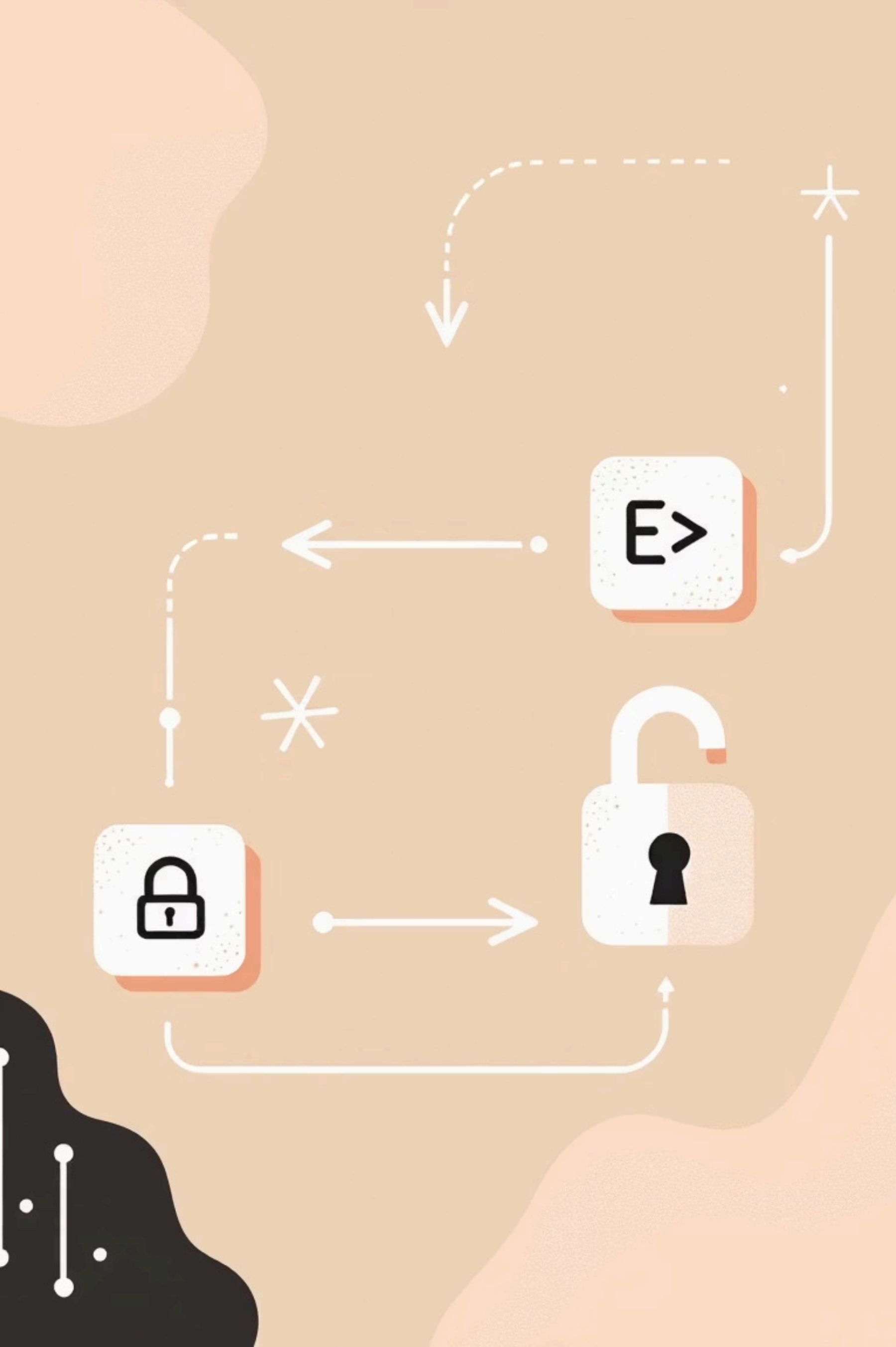
# Advanced Cryptanalysis using Neuro-Symbolic and Energy-Based Analysis

Exploring Hybrid AI Approaches in Modern Cryptography



# Introduction to Cryptography

1

### Cryptography Defined

The science of securing communication using mathematical keys and ciphers to ensure confidentiality and integrity.

2

### Role of Cryptanalysis

The art and science of breaking ciphers and identifying weaknesses in cryptographic systems to assess their strength.

3

### Real-World Applications

Essential for secure banking, military communications, and daily internet security (HTTPS).

# Data Encryption Standard (DES)

## Core Structure

- Block cipher using a **Feistel structure** for encryption and decryption.
- Employs a 56-bit key and 16 rounds of processing.
- Strengths: Historically significant, simple to implement.

## Limitations

- Small key size renders it **vulnerable to brute-force attacks** by modern computing power.
- Primarily used for legacy systems due to security concerns.

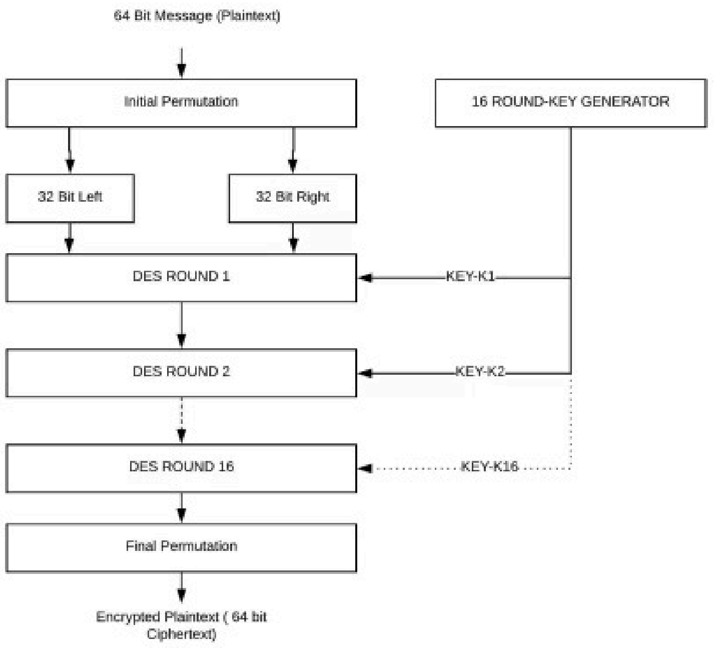
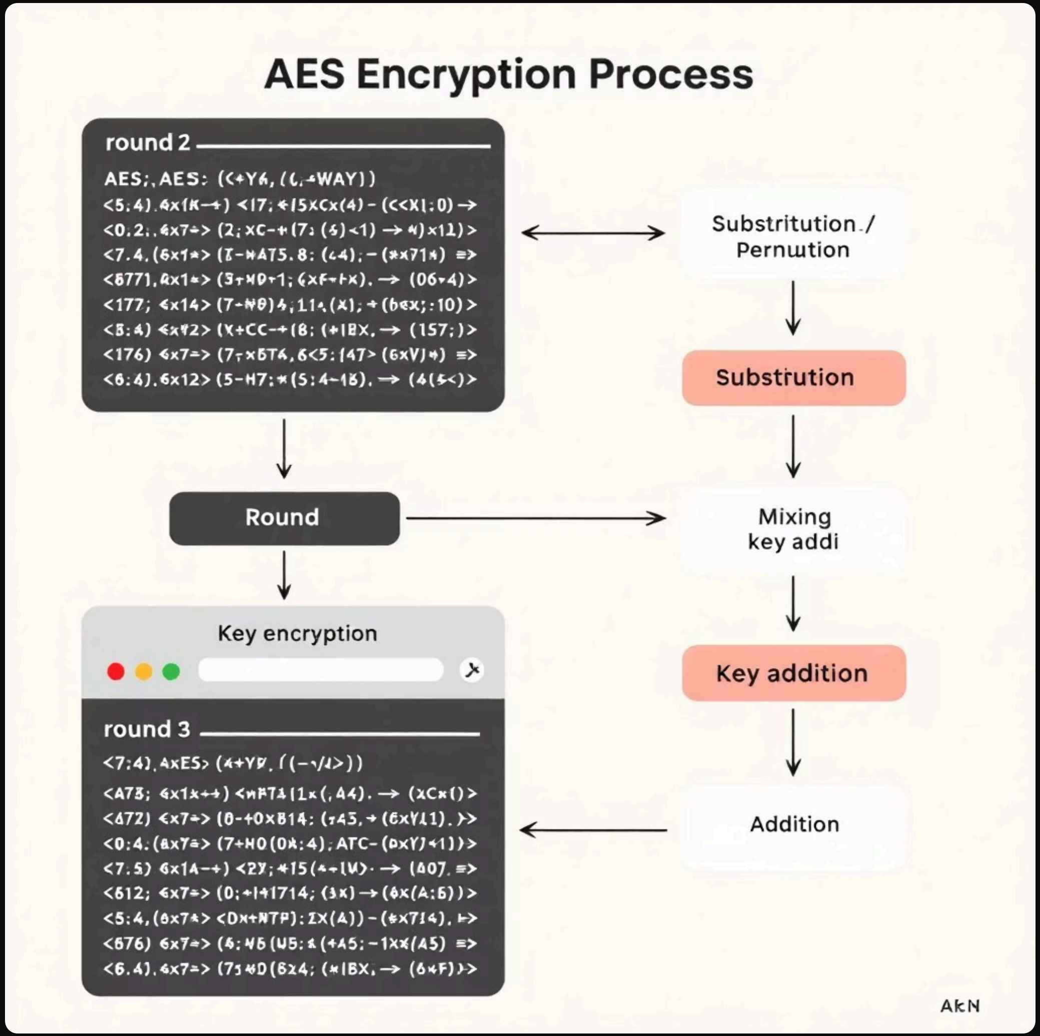


Figure 2.7: A pictorial view of DES algorithm

# Advanced Encryption Standard (AES)



## Key Characteristics

- Symmetric-key block cipher with 128, 192, or 256-bit keys.
- Iterative process involving multiple rounds of transformations.
- Strengths: Highly secure, widely adopted, resistant to classical attacks.

## Vulnerabilities

- Susceptible to **side-channel attacks** (e.g., power analysis, timing attacks).
- Potential for **AI-driven cryptanalysis** to exploit subtle patterns.

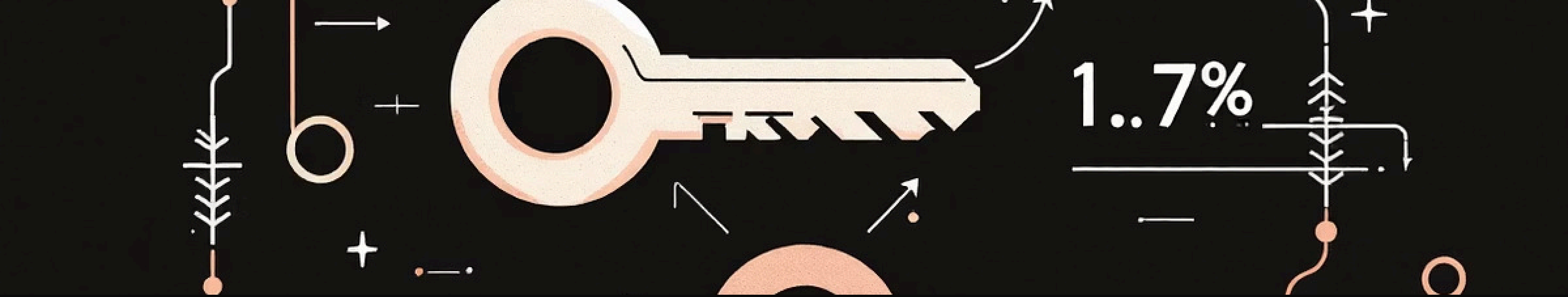
# AES vs DES: A Cryptographic Comparison

## AES (Advanced Encryption Standard)

- **Type:** Symmetric block cipher (128/192/256-bit keys).
- **Operation:** Multiple rounds of substitution, permutation, mixing, and key addition.
- **Strengths:** Fast, highly secure, resistant to brute-force attacks.
- **Usage:** VPNs, Wi-Fi (WPA2/WPA3), cloud security.

## DES (Data Encryption Standard)

- **Type:** Symmetric block cipher (56-bit key).
- **Operation:** Based on Feistel structure with 16 rounds.
- **Strengths:** Historically significant, simple design.
- **Weaknesses:** Vulnerable to modern brute-force attacks (cracked in < 24 hours).



# RSA: The Asymmetric Cornerstone

### Asymmetric Encryption

Utilises a public-private key pair for encryption and decryption.

### How it Works

Public key encrypts data, while the corresponding private key decrypts it.

### Key Strengths

Secure for key exchange, digital signatures, and foundational for SSL/TLS.

### Limitations

Slower for large data encryption; requires large key sizes (2048+ bits) for security.

**Real-world Use:** Online banking, HTTPS, secure email.

# ECC: Efficiency in Asymmetric Cryptography

### Elliptic Curve Math

Based on complex mathematics of elliptic curves over finite fields.

### Strength & Key Size

Offers equivalent security with significantly smaller key sizes (e.g., 256-bit ECC ≈ 3072-bit RSA).

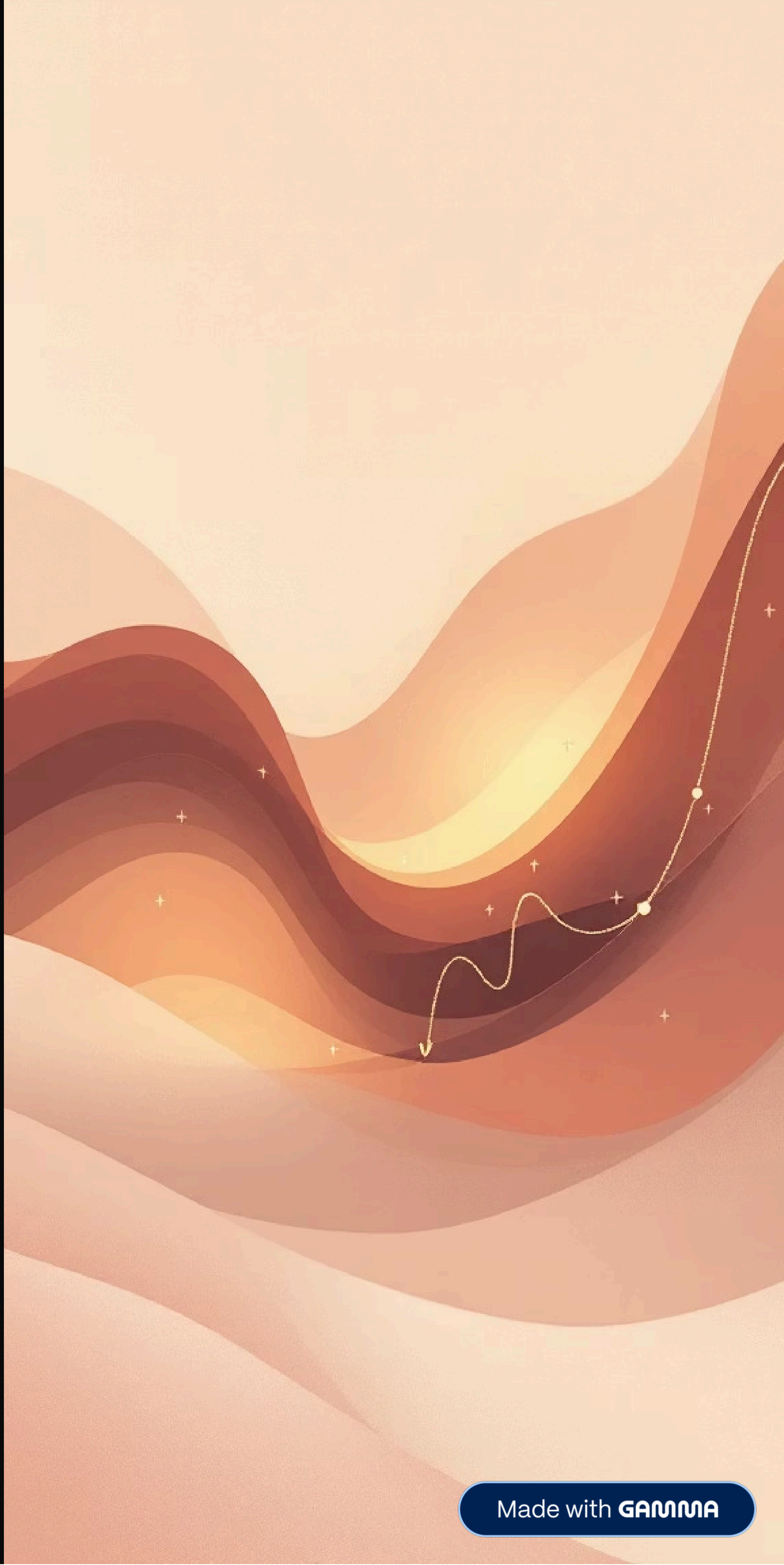
### Efficiency & Use Cases

Lightweight and efficient, ideal for IoT devices and mobile applications.

### Challenges

More complex mathematics and less widespread adoption compared to RSA.

**Real-world Use:** Cryptocurrency wallets, secure messaging (Signal, WhatsApp).



# Encryption Modes: ECB vs. CBC

Understanding how block ciphers operate on data blocks.

## Electronic Codebook (ECB)

Each block of plaintext is encrypted independently using the same encryption key.

- Simple: Straightforward to implement and parallelize.
- Pattern Vulnerability: Identical plaintext blocks produce identical ciphertext blocks, revealing patterns.
- No Error Propagation: An error in one block only affects that block.

## Cipher Block Chaining (CBC)

Each plaintext block is XORed with the previous ciphertext block before being encrypted. An Initialization Vector (IV) is used for the first block.

- Pattern Hiding: Eliminates plaintext patterns by chaining dependencies.
- Randomized Output: IV ensures that identical plaintext encrypted multiple times produces different ciphertexts.
- Error Propagation: An error in one ciphertext block affects the decryption of subsequent blocks.

## Relevance for Cryptanalysis Projects

### ECB for Basic Analysis

Due to its pattern-revealing nature, ECB is often ideal for introductory cryptanalysis projects

### CBC for Advanced Analysis

CBC's robust pattern hiding makes it more challenging for cryptanalysis.

# Convolutional Neural Networks (CNN)

CNNs are a class of deep neural networks, primarily used for analyzing visual imagery and are highly effective at detecting patterns.

### Convolutional Layer

Applies filters to input data, creating feature maps that detect patterns like edges, textures, or more complex shapes.

### Pooling Layer

Reduces the dimensionality of feature maps, minimizing computational cost and making the network more robust to variations in input.

### Fully Connected Layer

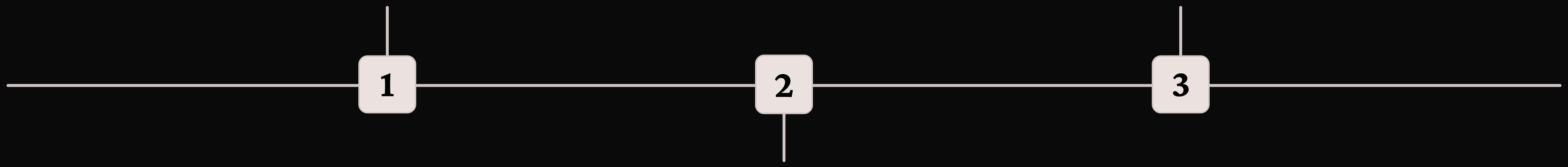
Interprets the learned features from previous layers to perform classification or regression tasks.

## Relevance to Cryptanalysis

CNNs can be applied in cryptanalysis to identify subtle patterns in ciphertext, detect anomalies in encrypted data, or analyze side-channel traces for information leakage.

# RNNs in Cryptanalysis

Recurrent Neural Networks (RNNs) are a powerful tool for analyzing sequential data, making them highly relevant in the field of cryptanalysis.



### Ciphertext Patterns

RNNs can be used to identify and analyze patterns within ciphertext, helping researchers and analysts uncover vulnerabilities in encryption algorithms.

### Side-Channel Analysis

By processing power traces and other side-channel data, RNNs can assist in key recovery tasks, providing insights into the inner workings of cryptographic systems.

### Key Recovery

RNNs have shown promise in tackling key recovery challenges, leveraging their ability to learn complex relationships within sequential data.

While RNNs are powerful, they do face certain challenges, such as training instability and the need for large amounts of data. Nonetheless, their ability to analyze sequential information makes them a valuable tool in the field of cryptanalysis.

# Mini-Project Work - Anushka

# Mini-Project Work - Rishit

1)Implemented a RNN model to try and break DES encrpytion using 64-bit length plaintext,56-bit key

2)Tried implementing a LSTM Model for the same purpose as above

3)Started pre-processing datasets for Side-Channel Attacks

# Thank You

Made with GAMMA