AES Modes of Operation: ECB and Alternatives

Sujoy Maity
Roll No: CrS2409

september 2, 2025

1 Why ECB mode is insecure for general use

ECB (Electronic Codebook) mode encrypts each block of plaintext independently using the same key. This simplicity makes it **insecure** for most practical applications because:

- **Pattern leakage:** Identical plaintext blocks produce identical ciphertext blocks. This can reveal patterns in the data, which can be exploited by attackers. For example, encrypting an image with ECB shows a visible outline of the original image.
- **No diffusion between blocks:** ECB does not mix information across blocks, so modifications to one block do not affect others, making it vulnerable to block rearrangement attacks.
- **Deterministic:** Encrypting the same message multiple times results in the same ciphertext, which makes it easier to detect repeated messages.

Conclusion: ECB is generally only suitable for very small, non-repeating data or random keys; for normal data, it is unsafe.

2 Recommended mode instead and why

More secure alternatives include **CBC (Cipher Block Chaining)**, **CTR (Counter)**, or **GCM (Galois/Counter Mode)**. Among these, **GCM** is often recommended.

- **CBC (Cipher Block Chaining):** Each plaintext block is XORed with the previous ciphertext block before encryption. This hides patterns and makes repeated blocks appear differently. Requires an **initialization vector (IV)** for the first block.
- **CTR (Counter mode):** Converts a block cipher into a stream cipher by encrypting a counter and XORing it with plaintext. Provides parallel encryption and random access to blocks. Requires a **unique nonce**.
- **GCM (Galois/Counter Mode):** Combines CTR mode encryption with a message authentication code (MAC) for integrity verification. It ensures **confidentiality and authenticity**, making it suitable for modern secure communications.

Recommendation: Use **AES-GCM**, because it provides both encryption and authentication, prevents pattern leakage, supports parallel processing, and is widely used in secure protocols like TLS.