

1. Introduction

AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) is a modern encryption algorithm widely used in secure communication systems. It provides confidentiality through encryption and integrity through authentication, making it ideal for banking, military, cloud storage, Wi-Fi encryption and TLS security.

2. Why ECB Mode is Insecure

Electronic Codebook (ECB) mode encrypts each block independently. This results in repeated plaintext blocks producing identical ciphertext blocks, allowing pattern visibility and making the encryption vulnerable to analysis. The absence of randomness and resistance to block manipulation makes ECB unsafe for sensitive or structured data.

3. Recommended Mode: AES-GCM

AES-GCM is preferred over ECB and older modes due to its high efficiency, authenticated encryption capability and wide industry adoption. GCM internally uses counter mode for speed and parallel processing while employing the Galois field for authentication.

4. Advantages of AES-GCM Mode

Feature	Benefit
Authenticated Encryption (AEAD)	Provides confidentiality + prevents data tampering.
High Performance	Fast due to parallelism and hardware acceleration.
Additional Authenticated Data (AAD)	Metadata can be verified without encryption.
No Padding Required	Accepts any message length securely.
Unique Nonce Usage	Prevents pattern repetition in output.
Industry Wide Adoption	Used in HTTPS, TLS 1.3, VPNs, Wi-Fi security, Cloud storage.

5. Conclusion

AES-GCM offers strong security by combining encryption with authentication. It overcomes limitations of ECB mode and ensures high performance, making it the preferred choice for modern cryptographic systems. Due to its reliability, speed, and validated industry trust, AES-GCM should be used for secure data transmission and storage where confidentiality and integrity are essential.