Real-Life Scenario: Secure Data Transmission for Healthcare Providers

Scenario Overview: A healthcare provider (e.g., a hospital or clinic) collects sensitive patient data, including medical records, test results, and treatment history. This data needs to be securely transmitted between different departments, as well as to external partners (e.g., insurance companies, research organizations) for further analysis or reimbursement. The current system uses AES-128 in ECB mode, but it has been identified that this method is insecure. The hospital needs to upgrade its encryption system to ensure that patient data remains confidential and can be securely shared.

The goal is to switch to AES-256 in GCM mode for stronger encryption and authentication, and add digital signatures to verify the integrity and authenticity of the data.

Before Mid-Term: Using AES-128 in ECB Mode

Problem:

The healthcare provider uses AES-128 in ECB mode for encrypting patient data. However, AES-ECB does not provide any form of data integrity or protection from patterns in data, making it vulnerable to attacks. If two identical records are encrypted, they would result in identical ciphertexts, which could reveal sensitive information about the data.

Plan:

Upgrade the encryption to AES-256 GCM for better security, and use a digital signature to guarantee the authenticity of the data.

After Mid-Term: Adding Digital Signatures

Goal:

The healthcare provider wants to ensure the integrity and authenticity of the patient data before it is sent to external partners (e.g., insurance companies or research organizations). This can be done using RSA digital signatures.

By signing the encrypted data with the provider's private RSA key, they can ensure that the recipient can verify the data's authenticity using the provider's public key.

Steps:

1. Generate RSA Key Pair: The healthcare provider generates a public/private RSA key pair.

2. Sign Encrypted Data: The provider signs the encrypted data with their private RSA key.

3. Verify Signature: The recipient (e.g., insurance company) can verify the signature using the public RSA key to ensure the data is from the healthcare provider and hasn’t been tampered with.