Cryptography

Modes of Block Cipher Operation

M S Vilkhu

02 Dec 2024 (C1/C3/C5)

Modes of Block Cipher Operation

- **Modes of Block Cipher Operation**
- Block ciphers are cryptographic algorithms that work on **fixed-size blocks** of data (e.g., 128 bits for AES). To encrypt or decrypt data **larger than a single block**, different **modes of operation** are used.
- These modes define **how plaintext blocks** are **processed** and how ciphertext blocks are generated, adding flexibility and security features to the cipher.

1. Electronic Codebook (ECB) Mode
2. Cipher Block Chaining (CBC) Mode
3. Cipher Feedback (CFB) Mode
4. Output Feedback (OFB) Mode
5. Counter (CTR) Mode
6. Galois/Counter Mode (GCM)

Types of Block Cipher Modes

- **Types of Block Cipher Modes**
- **1. Electronic Codebook (ECB) Mode**
- **How It Works:** Each plaintext block is **encrypted independently** using the same key.
- **Features:**
    - Simple and parallelizable.
    - Identical plaintext blocks produce identical ciphertext blocks, making it insecure for repetitive patterns.
- **Use Case:** Rarely used, mainly for small, independent data segments (e.g., encrypting random keys).
- **Security Risk:** Vulnerable to pattern recognition

Types of Block Cipher Modes

- **2. Cipher Block Chaining (CBC) Mode**
- **How It Works:**
  - Each plaintext block is **XORed with the previous** ciphertext block before encryption.
  - Requires an **Initialization Vector (IV) for the first block**.
- **Features:**
  - Adds **dependency** between blocks, making **patterns** in plaintext **less visible.**
  - Decrypting a block requires the preceding ciphertext block.
- **Use Case:** File encryption and secure communication.
- **Security Risk:** IV must be **unpredictable**; reusing IVs compromises security.

Types of Block Cipher Modes

- **3. Cipher Feedback (CFB) Mode**
- **How It Works:**
  - Converts a **block cipher into a stream cipher**.
  - Encrypts the previous ciphertext block (or IV for the first block) and **XORs the result with the plaintext** to produce ciphertext.
- **Features:**
  - Operates in smaller units (e.g., bits or bytes) for real-time data.
  - Decryption uses the same process as encryption.
- **Use Case:** Real-time encryption, such as for network streams.
- **Security Risk:** Similar IV precautions as CBC.

Types of Block Cipher Modes

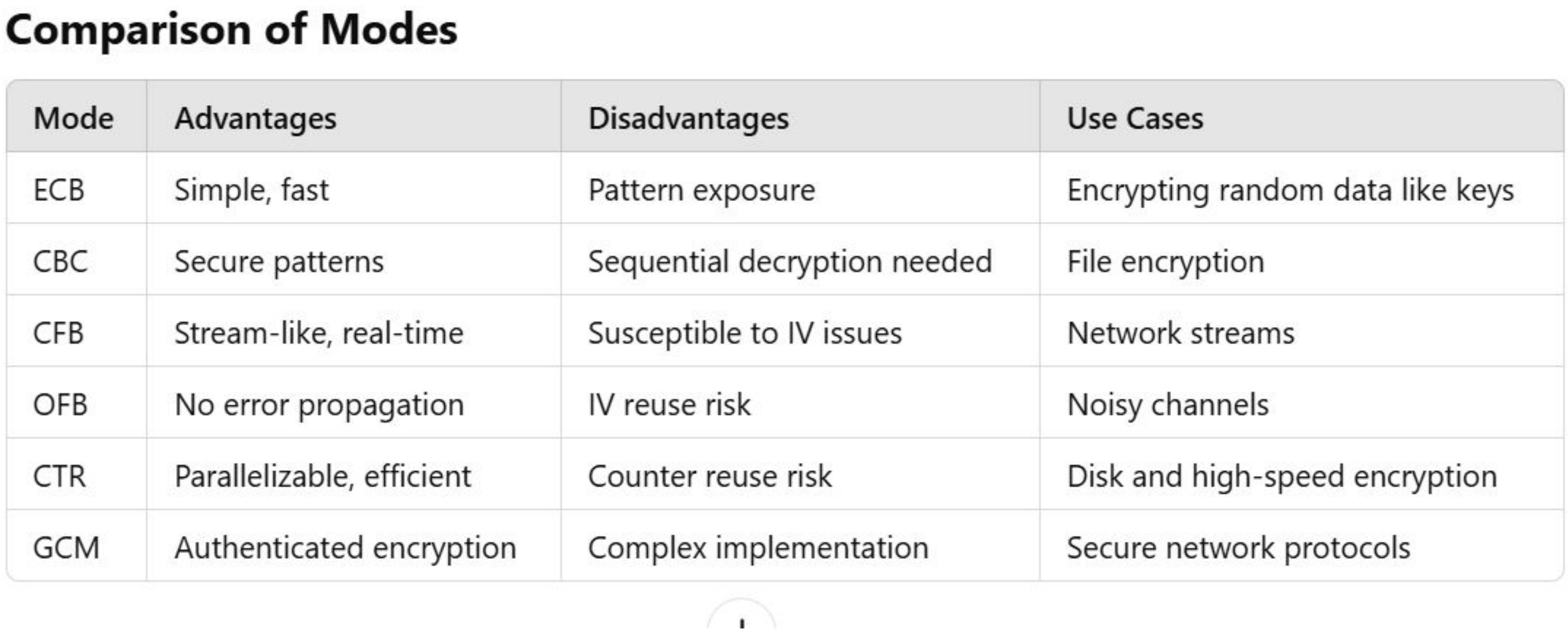
- **4. Output Feedback (OFB) Mode**
- **How It Works:**
  - Turns a **block cipher into a stream cipher** by generating a keystream.
  - The cipher's **output is fed back** into the encryption process, independent of the plaintext.
- **Features:**
  - Resistant to error propagation.
  - Requires synchronization between sender and receiver.
- **Use Case:** Encryption in noisy communication channels.
- **Security Risk:** Reuse of the IV compromises security.

Types of Block Cipher Modes

- **5. Counter (CTR) Mode**
- **How It Works:**
  - Uses a **counter value as input to the cipher**, incremented for each block.
  - The cipher's output is **XORed** with the plaintext to produce ciphertext.
- **Features:**
  - Highly parallelizable and efficient.
  - Works as a stream cipher.
  - No dependency between blocks.
- **Use Case:** High-performance applications, such as disk encryption.
- **Security Risk:** Counter values must not repeat.

Types of Block Cipher Modes

- **6. Galois/Counter Mode (GCM)**
- **How It Works:**
  - A **variant of CTR** mode that provides encryption and authentication.
  - Includes a **Galois field multiplier to compute a Message Authentication Code** (MAC).
- **Features:**
  - Combines confidentiality and integrity.
  - Efficient for parallel processing.
- **Use Case:** Authenticated encryption for secure network protocols (e.g., TLS, IPsec).
- **Security Risk:** Misuse of nonces (e.g., repetition) can compromise security.



Comparison of Modes

Mode	Advantages	Disadvantages	Use Cases
ECB	Simple, fast	Pattern exposure	Encrypting random data like keys
CBC	Secure patterns	Sequential decryption needed	File encryption
CFB	Stream-like, real-time	Susceptible to IV issues	Network streams
OFB	No error propagation	IV reuse risk	Noisy channels
CTR	Parallelizable, efficient	Counter reuse risk	Disk and high-speed encryption
GCM	Authenticated encryption	Complex implementation	Secure network protocols

Thank You