Block Cipher

Eighth lecture

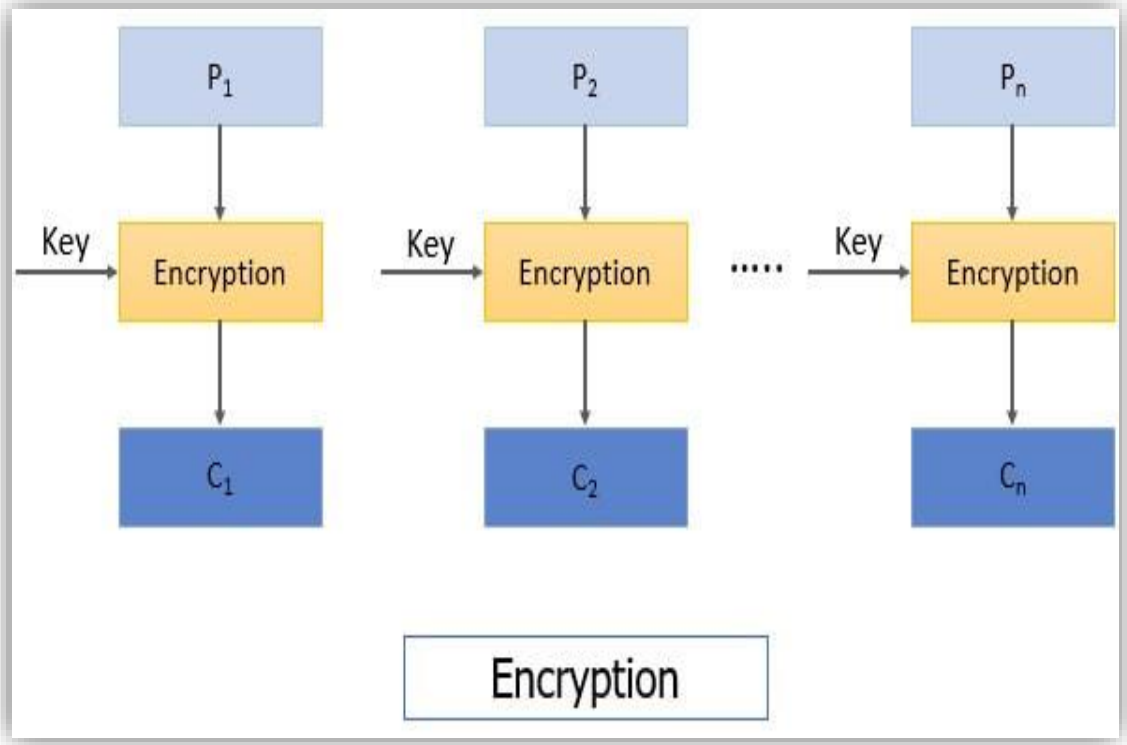
By: Assist Prof. Dr. Saja J. Mohammed

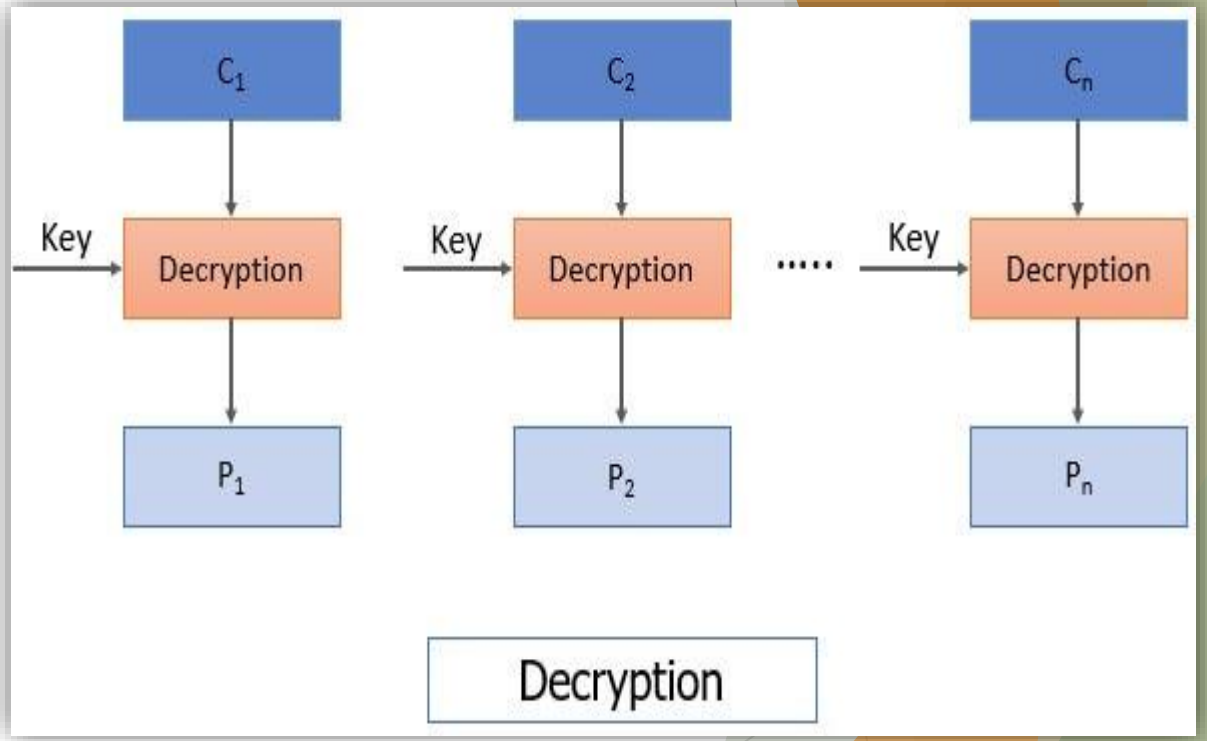
2024-2025

What is a block cipher?

- A **block cipher** is a **symmetric cryptographic technique** which we used to **encrypt a fixed-size data block using a shared, secret key.**
- The block cipher processes fixed-size blocks **simultaneously**, as opposed to a stream cipher, which encrypts data one bit at a time.
- Most modern block ciphers are designed to encrypt data in fixed-size blocks of either 64 or 128 bits.
- A block cipher requires an **initialization vector (IV) (**is derived from a random number generator**)** that is added in order to make it more difficult to **use brute force to break the key.**
- In block ciphers, the **S-boxes and P-boxes** are used to make the relation between the plaintext and the ciphertext difficult to understand.
- The popular variations of the block cipher algorithm include the **Data Encryption Standard (DES), Triple DES,** and the **Advanced Encryption Standard (AES).**

Block cipher principle





Stream cipher vs block cipher

Stream Cipher	Block Cipher
Stream cipher operates on smaller Units of Plaintext	Block cipher operates on larger block of data
Faster than block cipher	Slower than Stream Cipher
Stream cipher processes the input element continuously producing output one element at a time	Block cipher processes the input one block of element at a time, producing an output block for each input block
Require less code	Requires more code
Only one time of key used.	Reuse of key is possible
Ex: One time pad	Ex: DES (Data Encryption Standard)
Application: SSL (secure connection on the web)	Application: Database, file encryption.
Stream cipher is more suitable for hardware implementation	Easier to implement in software.

Permutation box and substitution box

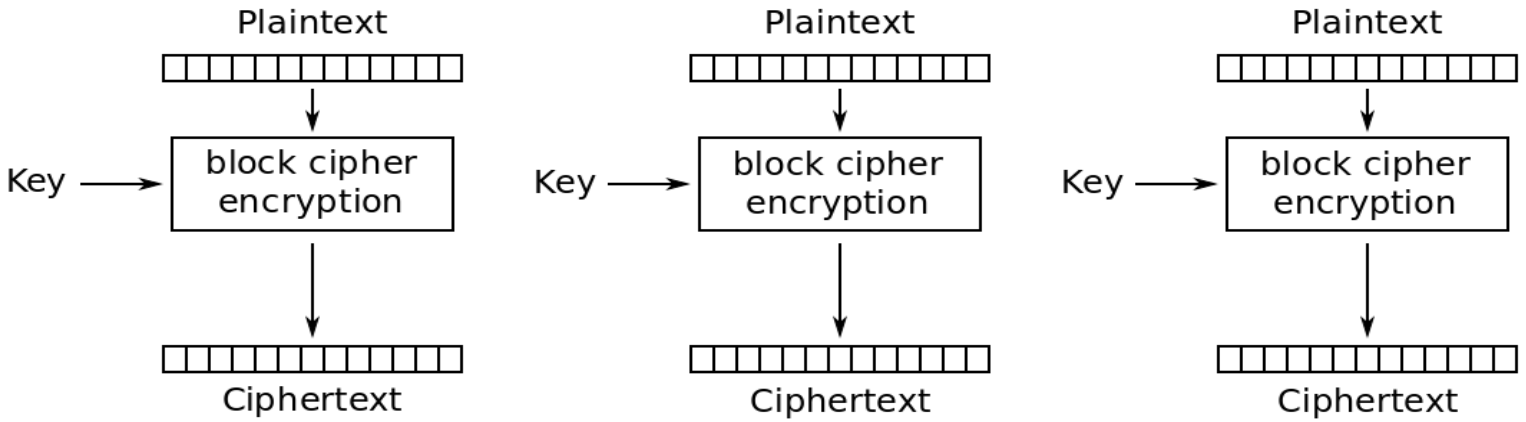
- **Permutation box (or P-box)** is a method of bit-shuffling used to permute or transpose bits across S-boxes inputs**.**
- P-boxes are typically classified as
  - **Compression:** the number of output bits is ***less than*** the number of input bits
  - **Expansion:** the number of output bits is ***greater than*** the number of input bits
  - **Straight :** the number of output bits is ***equal to*** the number of input bits.

- **Substitution-box(S-box)** is an another basic component of symmetric key algorithms which performs substitution. They are typically used in block cipher to hidden the relationship between the key and the ciphertext.
- In general, an S-box takes some number of input bits, *m*, and transforms them into some number of output bits, *n*, where *n* is not necessarily equal to *m*.

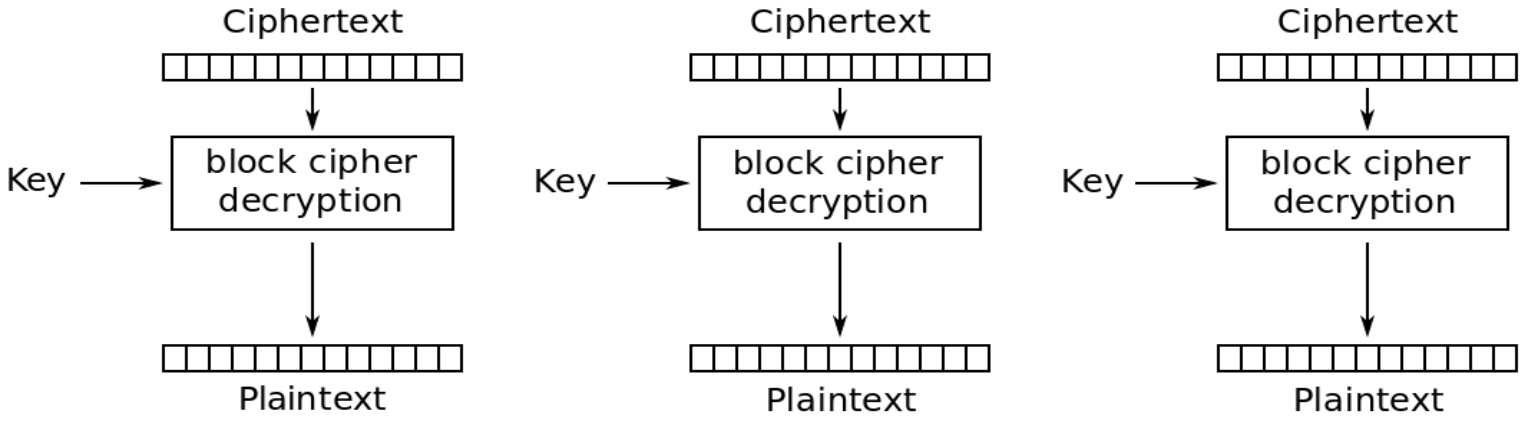
What are the different modes of operation in block cipher?

- A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.
- There are various modes of operation of a block cipher, for example:
  - Electronic Code Book (ECB) Mode.
  - Cipher Block Chaining (CBC) Mode.

Electronic Code Book (ECB) Mode

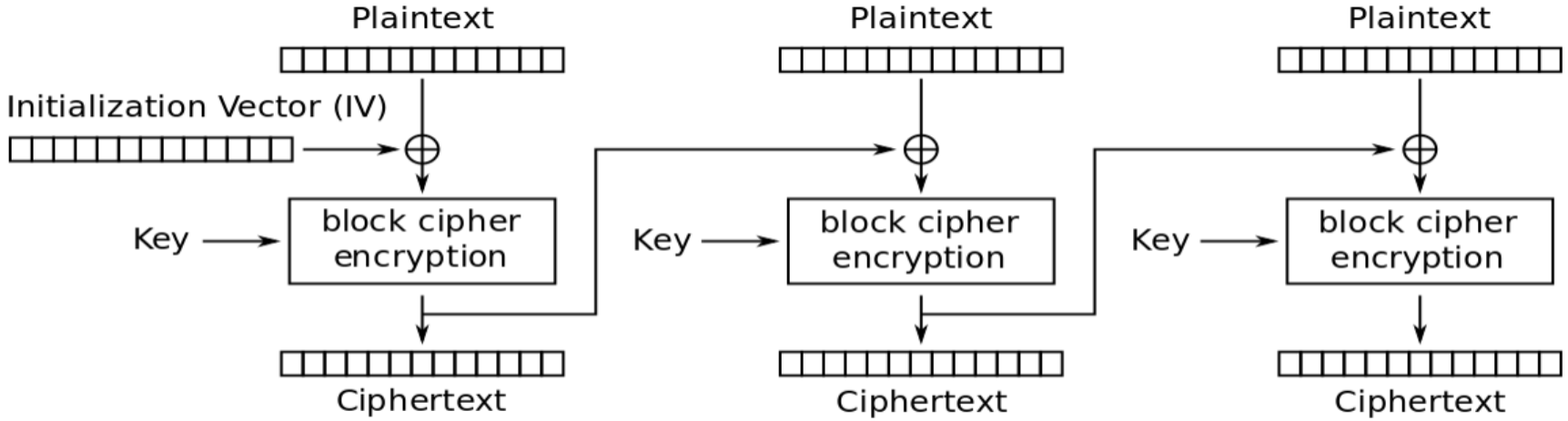


Electronic Codebook (ECB) mode encryption

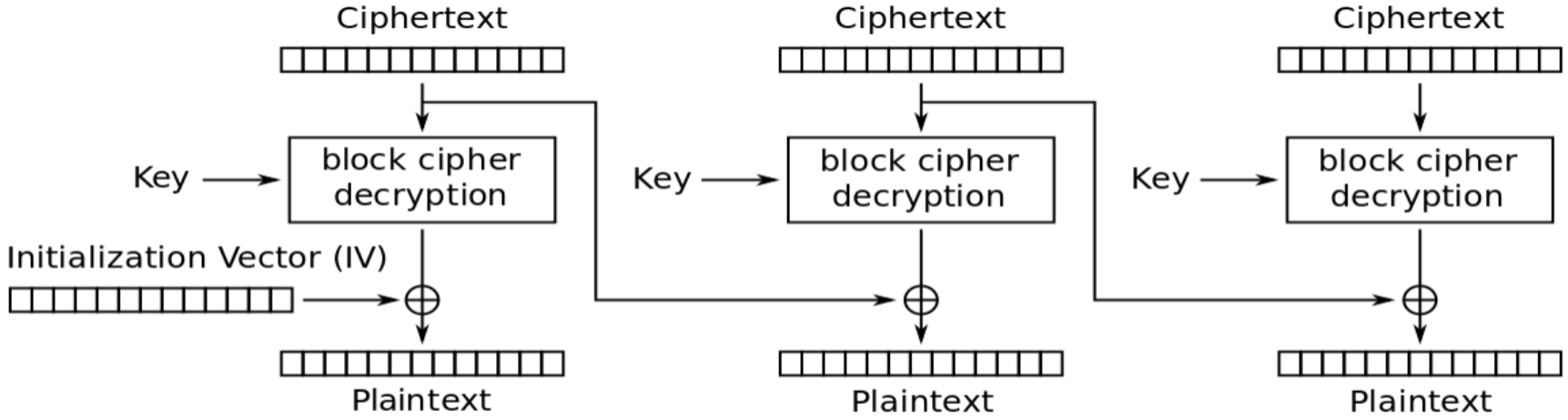


Electronic Codebook (ECB) mode decryption

Cipher Block Chaining (CBC) Mode



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption