



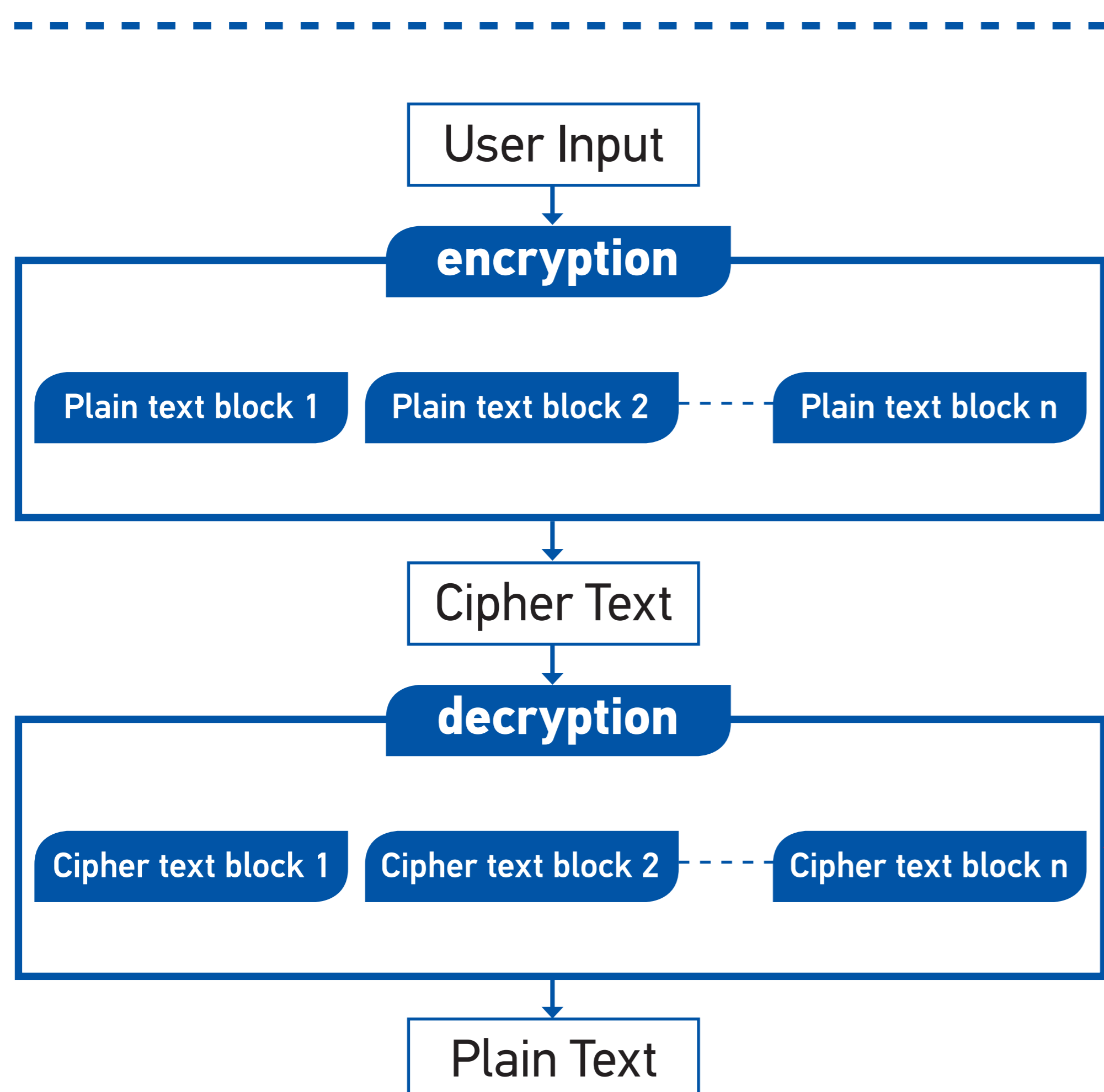
An Interactive Web Demo for Various Cipher Mode Operations

Objective

To develop an interactive web-based application that provides an educational tool which allows user to navigate through the various block cipher mode operations in the encryption and decryption process while not compromising ease of use.

Block Cipher

- Used in modern cryptography standards and are commonly found in symmetric key encryption techniques.
- Encrypts data one block at a time.
- Size of each block is fixed depending on the algorithm used.
- **First block to n-number of blocks**
- Each **block cipher operational mode** processes each individual data block differently, producing unique output.



TECHNOLOGIES USED



Visual Studios

- Web Development



Bootstrap

- UI/UX



Azure

- Web Deployment

OPERATIONAL MODES

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback Block (CFB)
- Output Feedback Block (OFB)
- Counter Block (CTR)

ALGORITHMS USED

- Advanced Encryption Standards (AES)
- Data Encryption Standards (DES)
- Blowfish

PROCESS FEATURE

- Displays the process happening in each mode.
- ASCII and Hexadecimal output