Block ciphers – Modes of Operation – Part 1

LESSON 22 OF 40

CRYPTOGRAPHY & NETWORK SECURITY

Block cipher -

Modes of Operation

BLOCK CIPHER - Modes of Operation

- For different types of messages, we need different modes of operation.
- The five modes of operation are;
    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

Electronic Codebook (ECB) Mode

- Simplest mode of operation.
- Plain text is divide into a number of fixed sized blocks.
- If message is not a multiple of block size, then padding is done.
- Takes one block at a time and encrypt it.
- Same key used for both encryption and decryption for each block.

Electronic Codebook (ECB) Mode

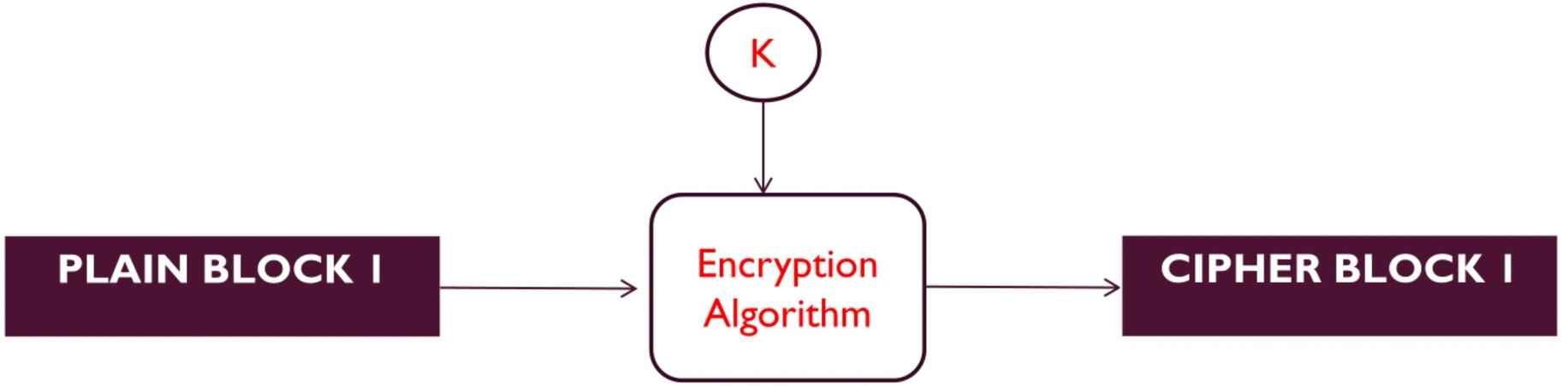
Let P = GREATMINDSTHINKALIKE

Let block size = 5

Electronic Codebook (ECB) Mode

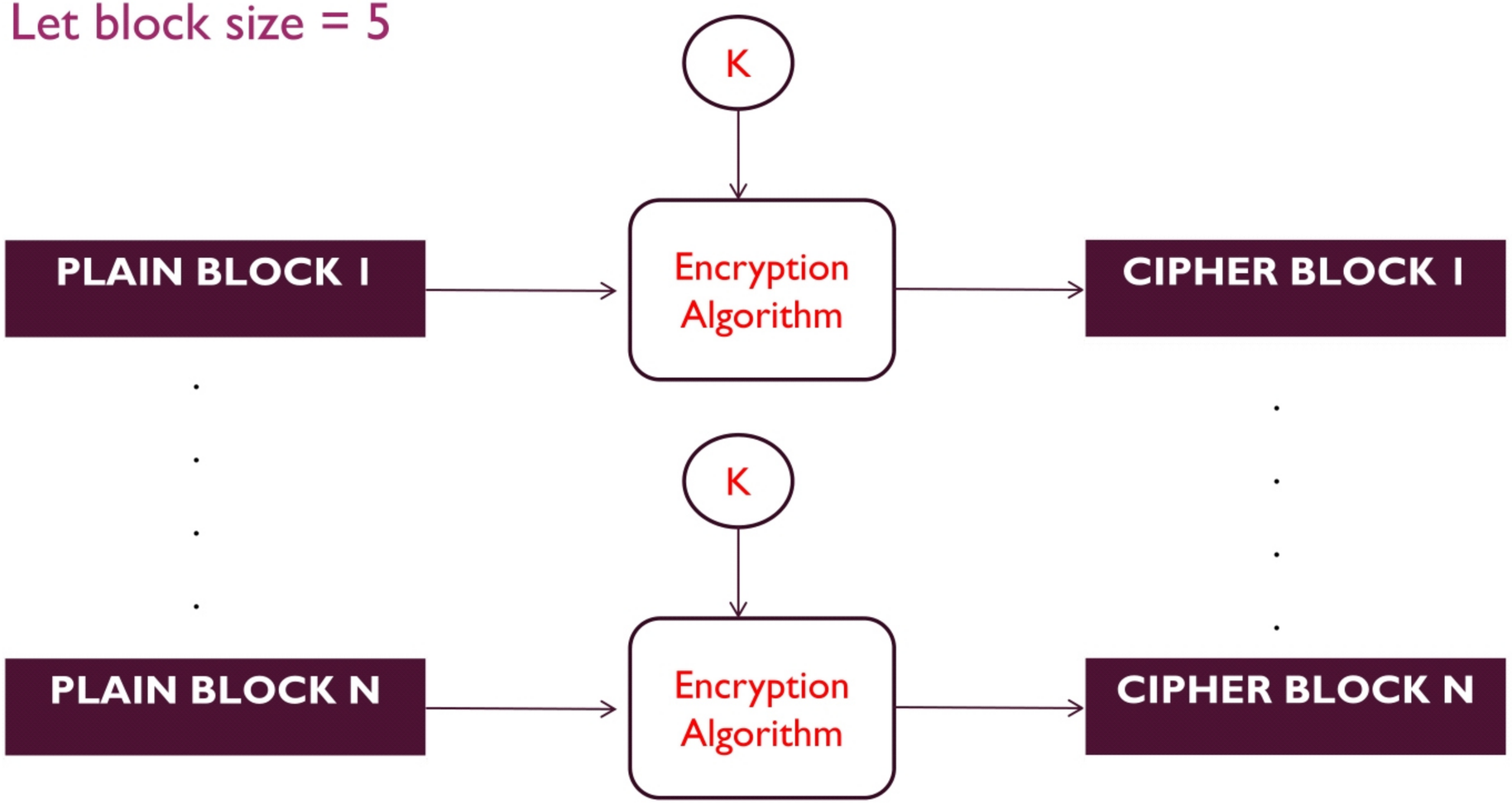
Let P = GREATMINDSTHINKALIKE
Let block size = 5

GREAT	MINDS	THINK	ALIKE
Block1	Block2	Block3	Block4



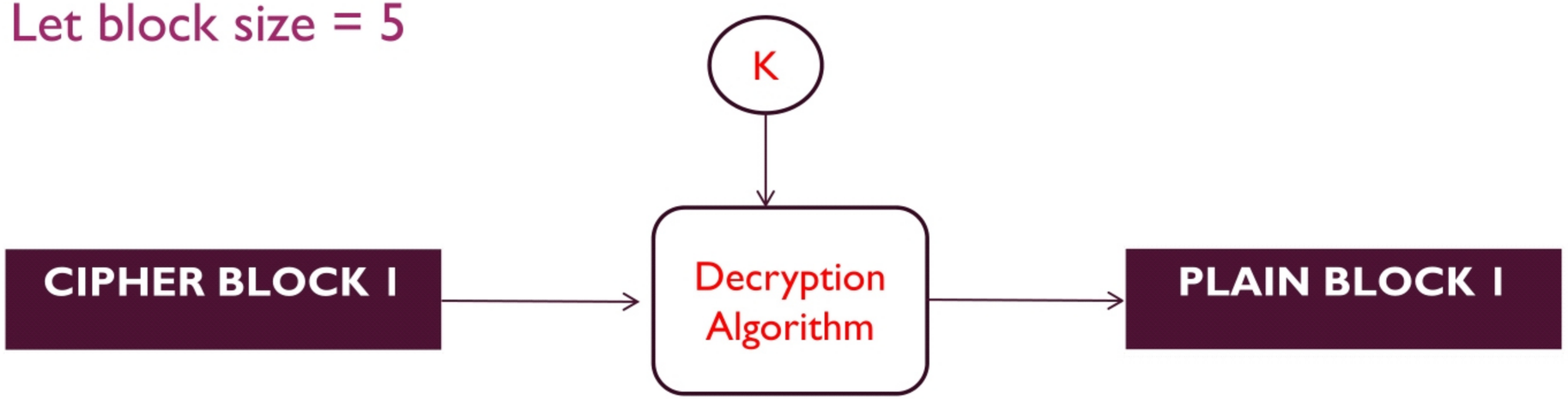
Electronic Codebook (ECB) Mode

Let P = GREATMINDSTHINKALIKE
Let block size = 5



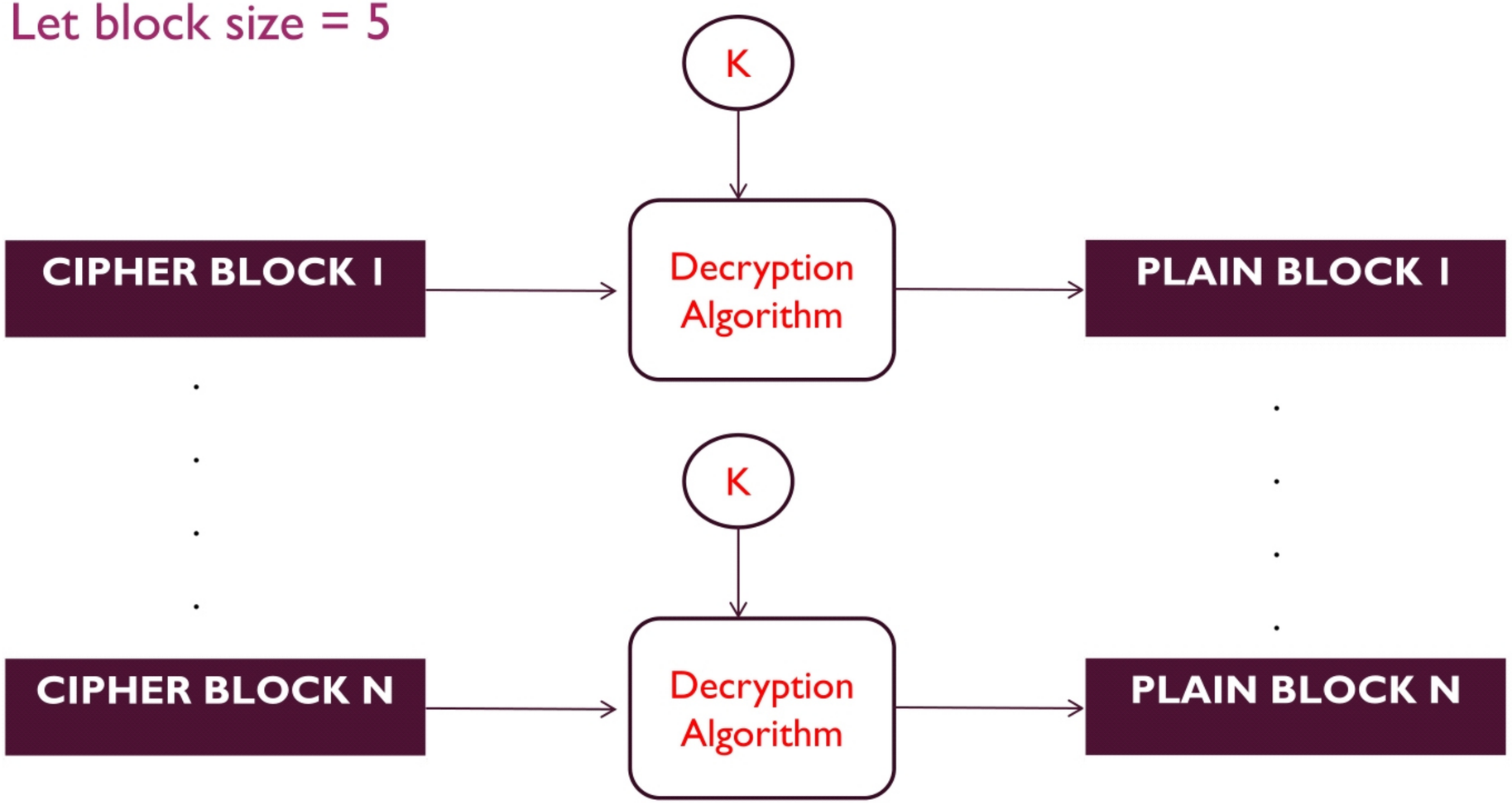
Electronic Codebook (ECB) Mode

Let P = GREATMINDSTHINKALIKE
Let block size = 5



Electronic Codebook (ECB) Mode

Let P = GREATMINDSTHINKALIKE
Let block size = 5



Electronic Codebook (ECB) Mode

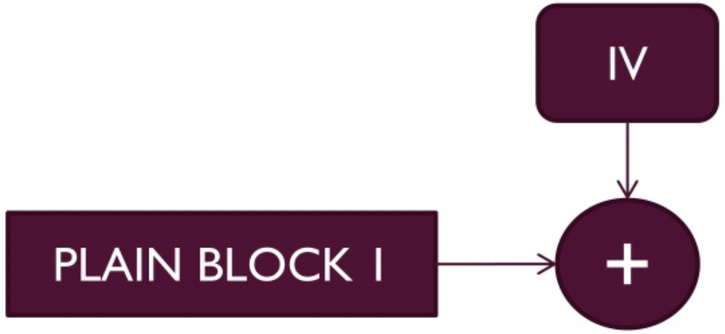
- Best for short amount of data, such as a key.
- Not secure for lengthy data.
- If identical blocks appear, then this mode produce same cipher text.

Cipher Block Chaining (CBC) Mode

- To overcome security issues of ECB Mode.
- The input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block.
- So repeating patterns are not exposed.
- Same key is used for encryption and decryption for each block.

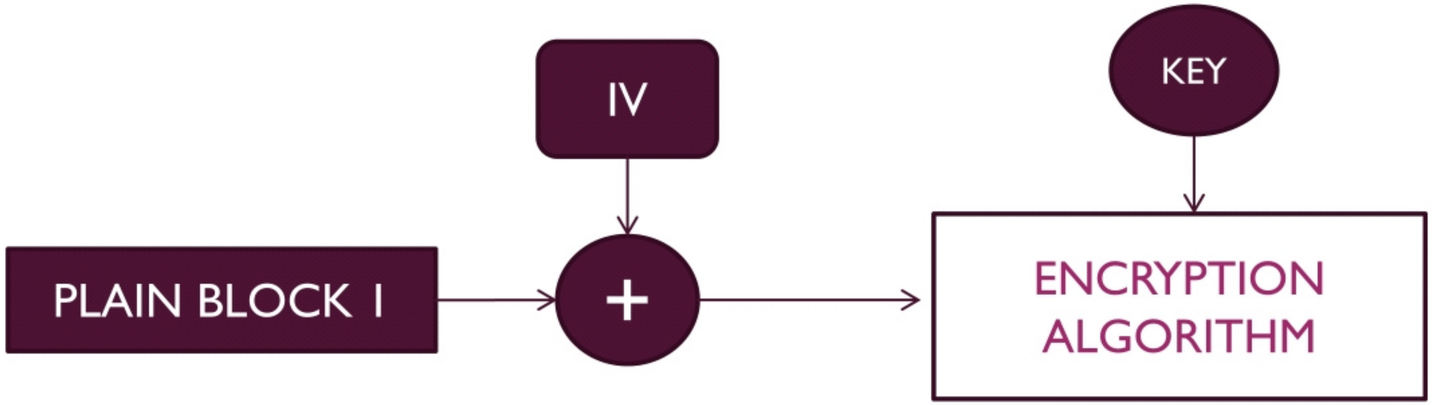
Cipher Block Chaining (CBC) Mode - Encryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.
- IV is a data block of same size.



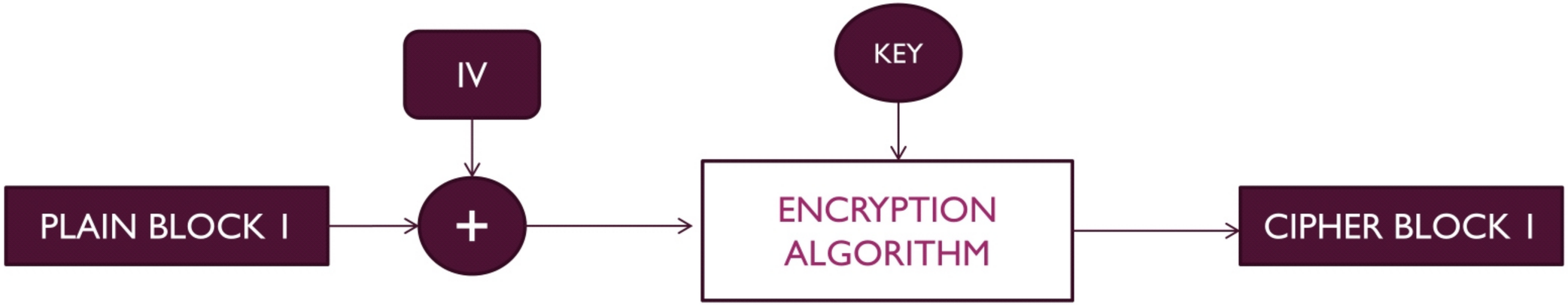
Cipher Block Chaining (CBC) Mode - Encryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



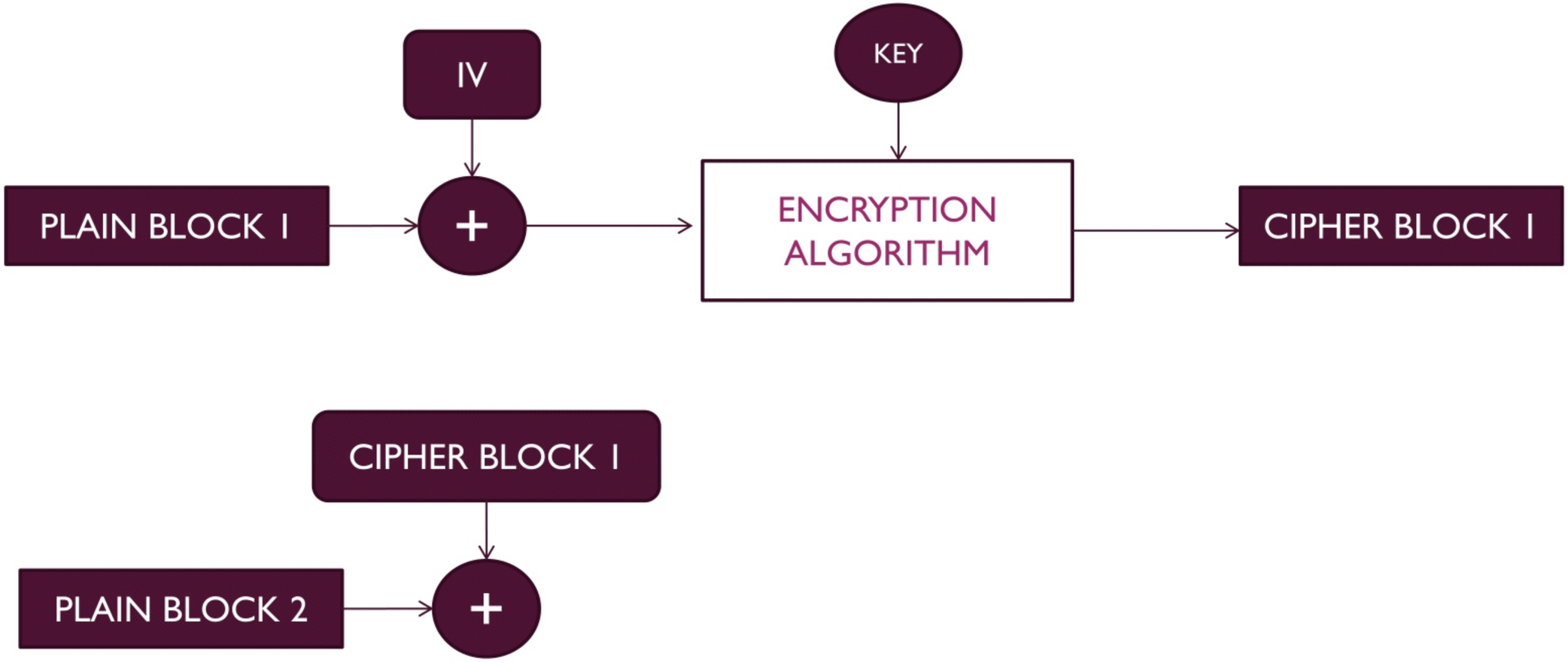
Cipher Block Chaining (CBC) Mode- Encryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



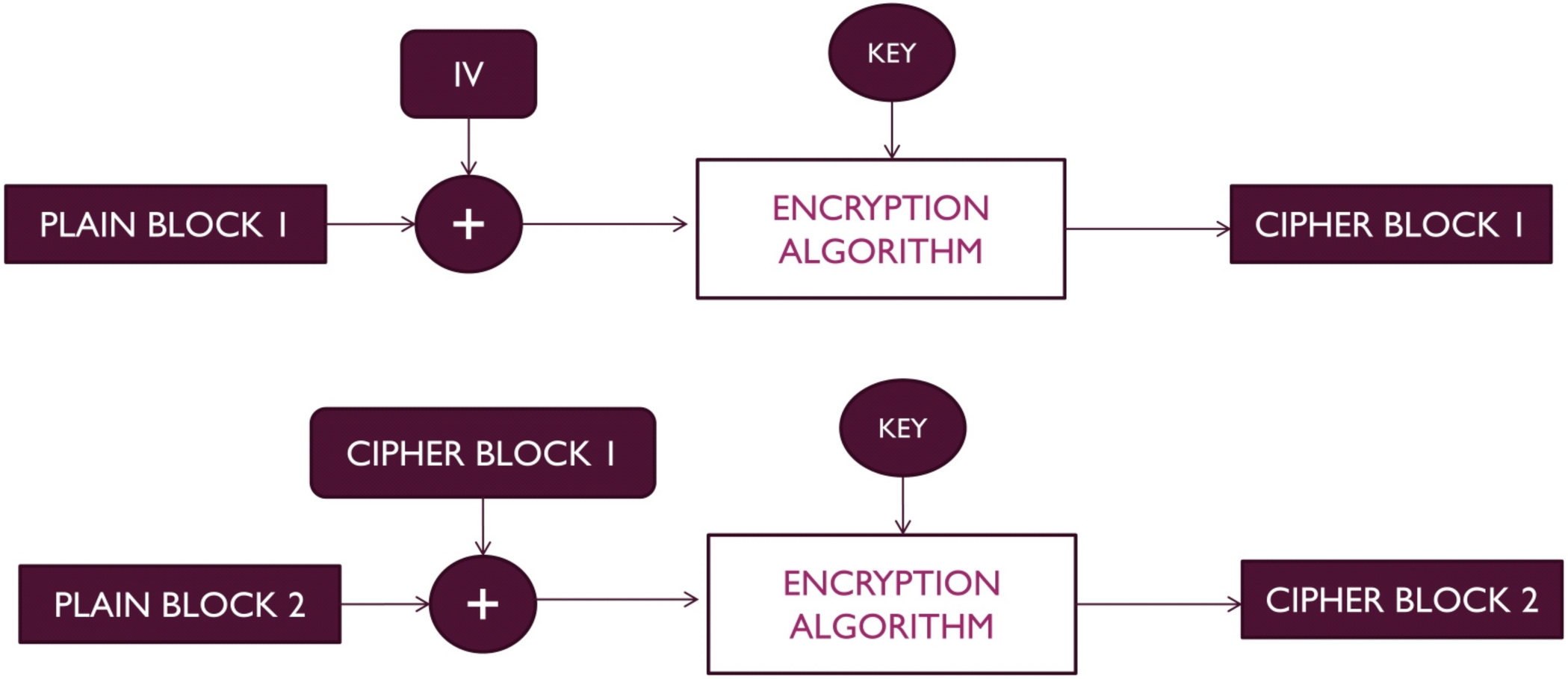
Cipher Block Chaining (CBC) Mode - Encryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



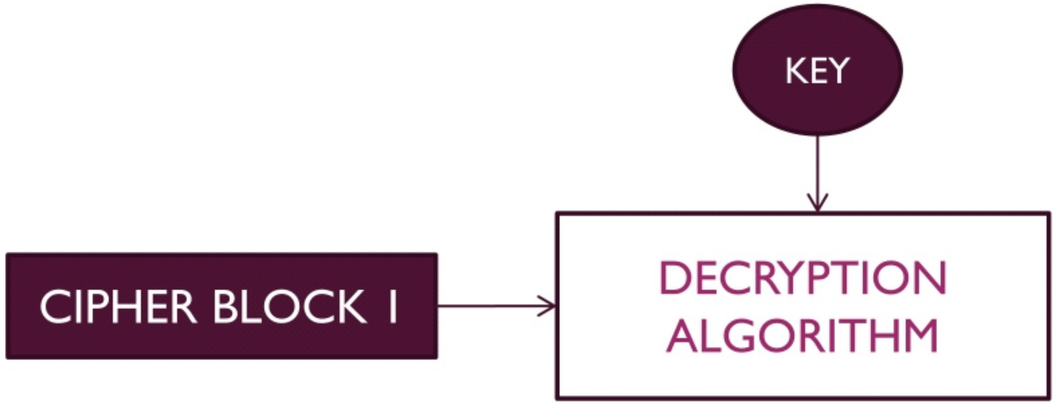
Cipher Block Chaining (CBC) Mode - Encryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



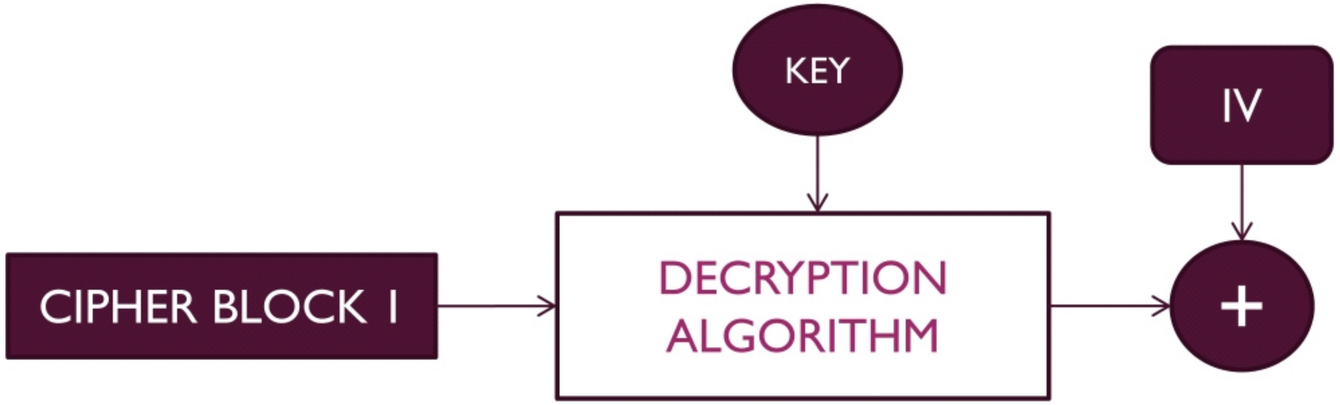
Cipher Block Chaining (CBC) Mode - Decryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



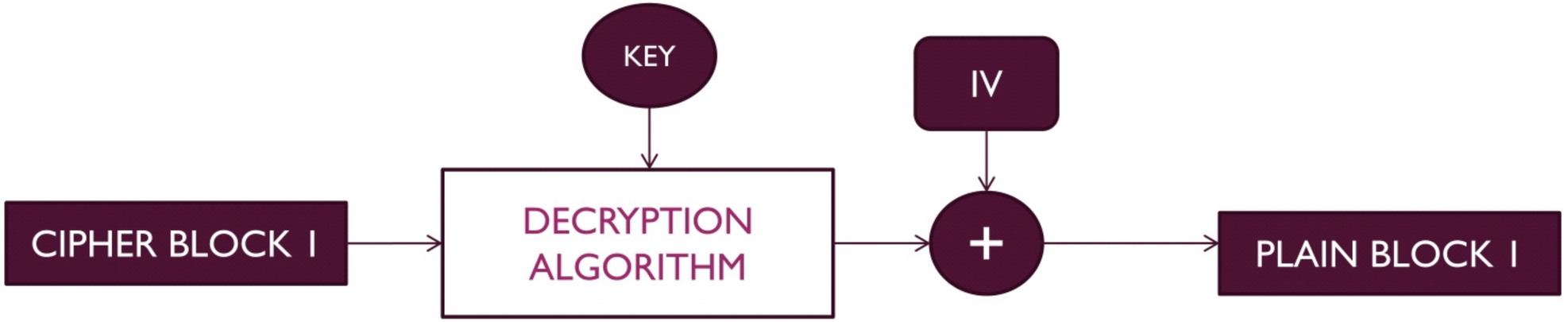
Cipher Block Chaining (CBC) Mode - Decryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



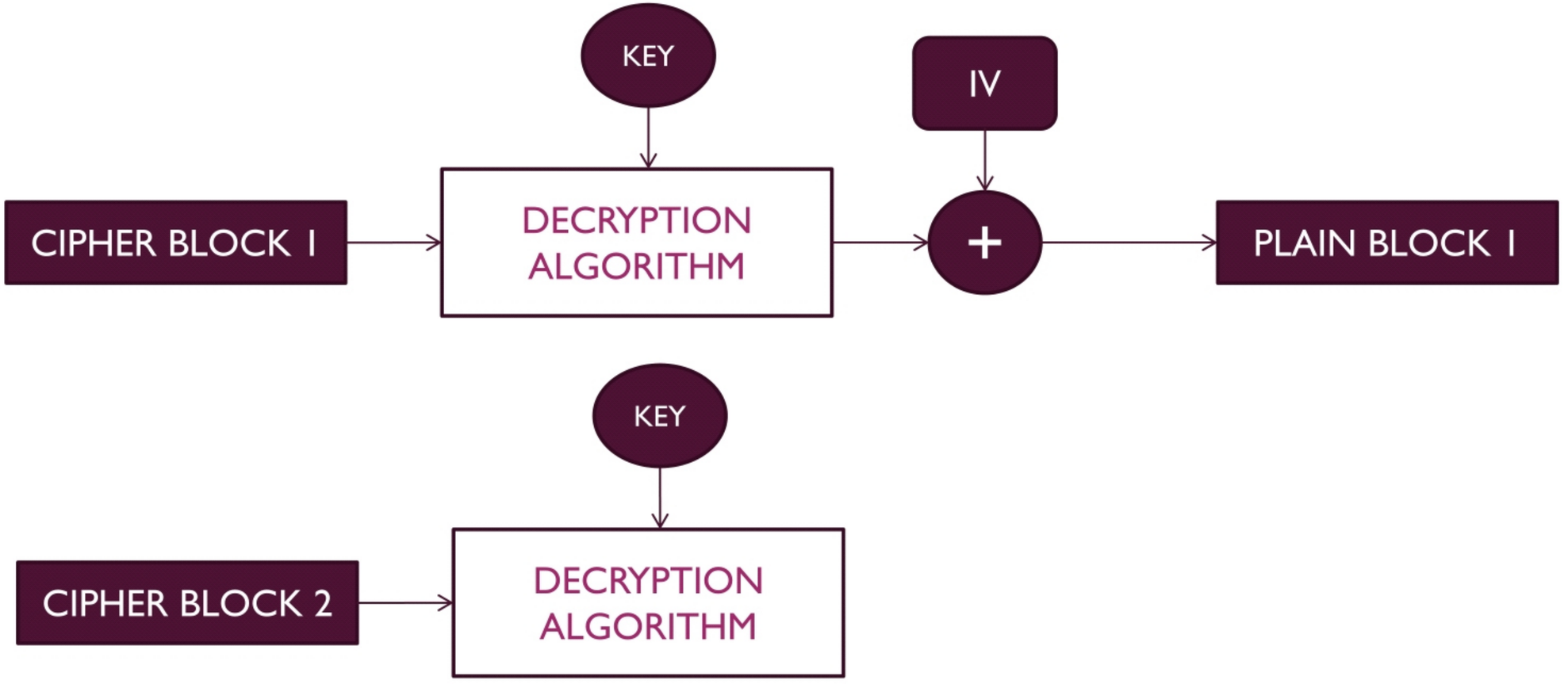
Cipher Block Chaining (CBC) Mode - Decryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



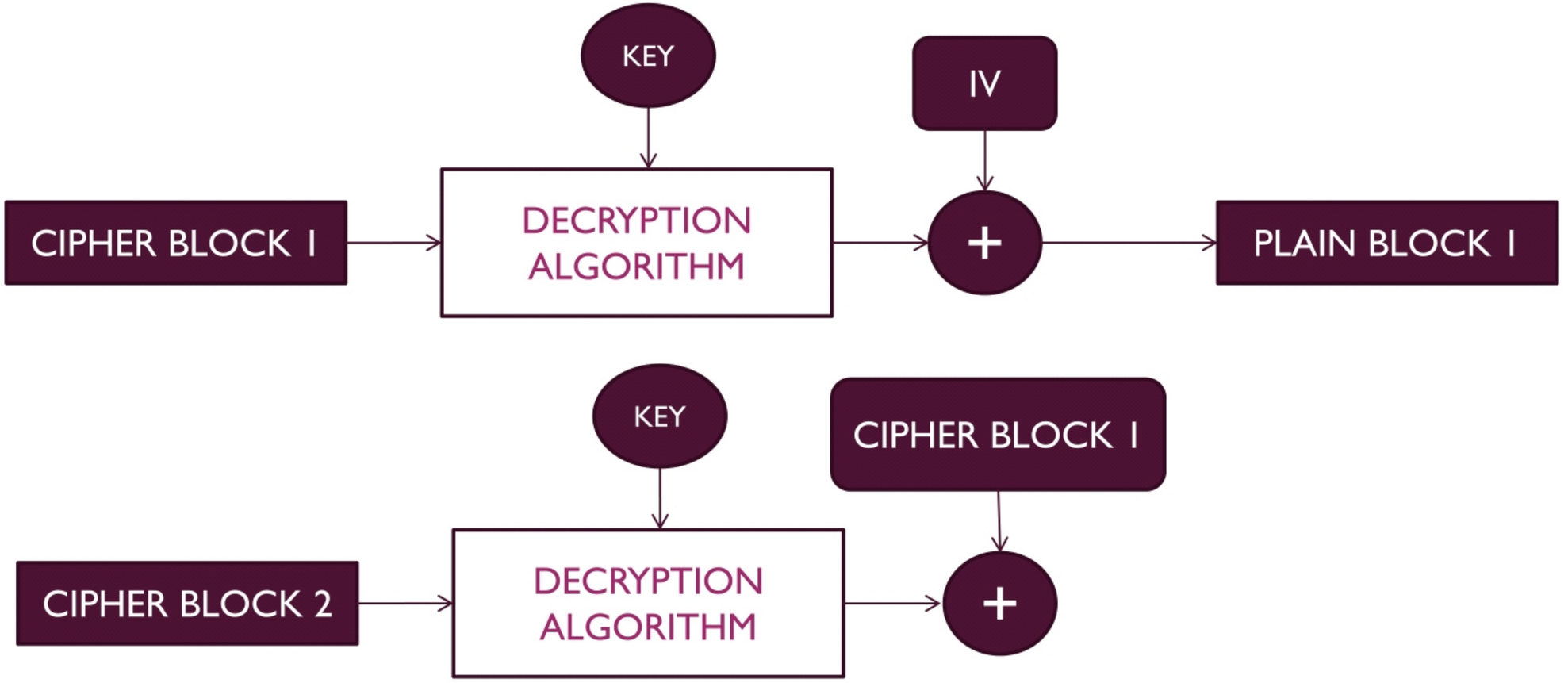
Cipher Block Chaining (CBC) Mode - Decryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



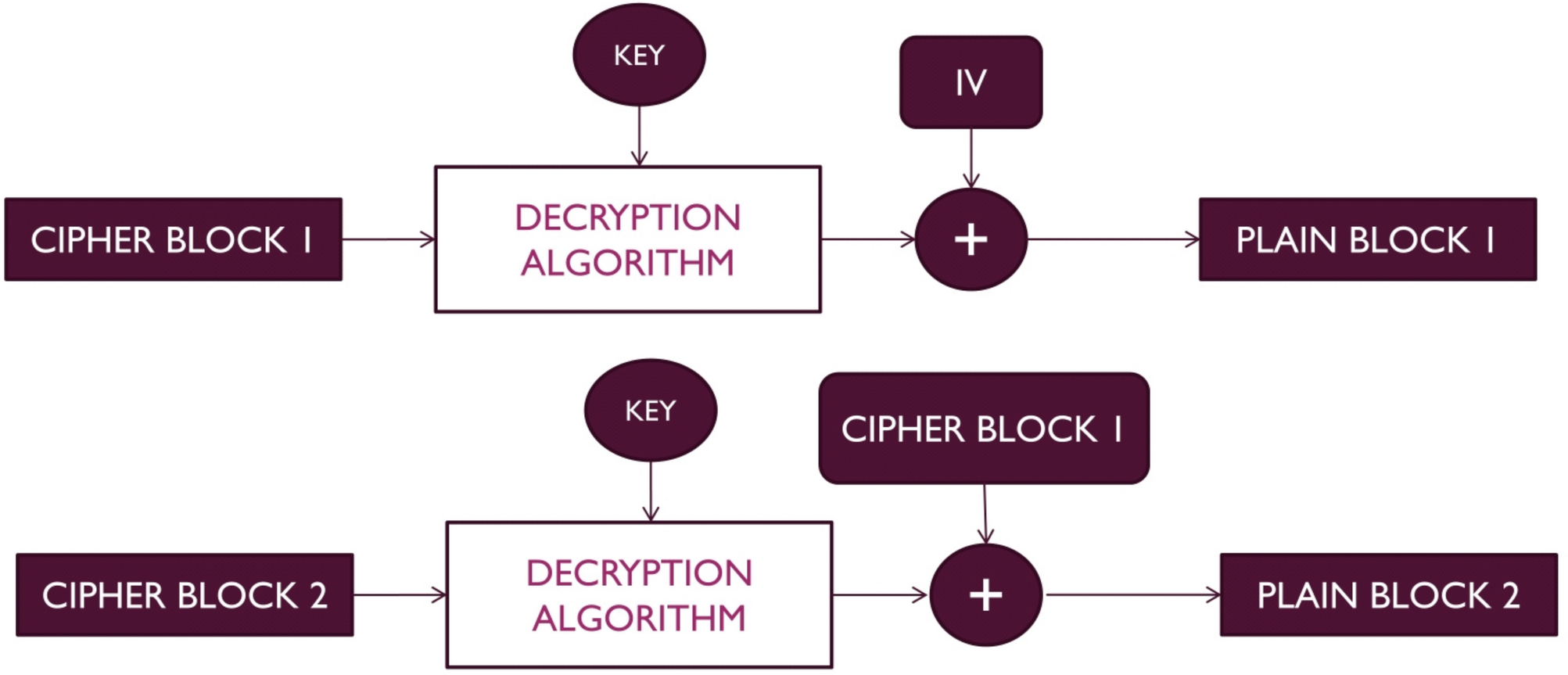
Cipher Block Chaining (CBC) Mode - Decryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



Cipher Block Chaining (CBC) Mode - Decryption

- An Initialization Vector (IV) is used in first encryption and fisrt decryption.



Cipher Block Chaining (CBC) Mode - Decryption

- IV must be known to both parties, but should be unpredictable by third parties.
- IV can be sent using ECB encryption to ensure maximum security.

- If we have two identical messages and if we use same IV, the cipher will also be same.

unacademy

Next to Study :

Block cipher Modes of operation.

Reference : Cryptography and Network Security Principles and Practices, Fourth Edition
By William Stallings

THANK YOU

PRESENTED BY,
ANSHA PK