CRYPTOGRAPHY & NETWORK SECURITY

Block cipher - Modes of Operation

Vijesh Nair

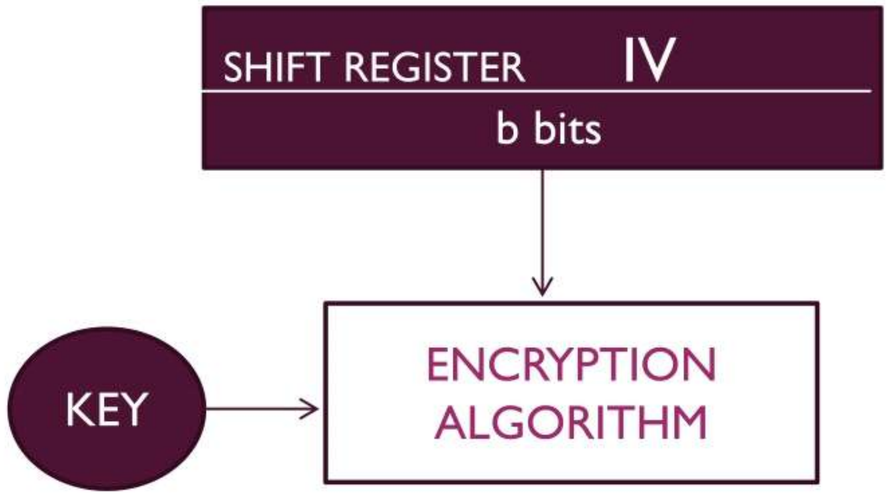
BLOCK CIPHER - Modes of Operation

- 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

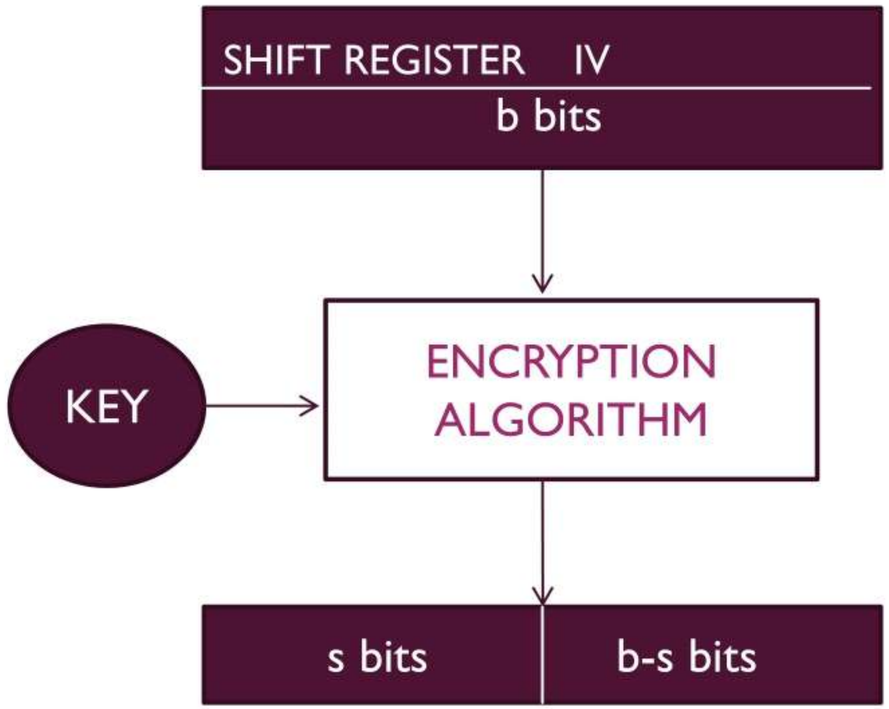
Cipher Feedback (CFB) Mode

- Block cipher as a stream cipher.
- Eliminates the need to pad a message to be an integral number of blocks.
- The plaintext is divided into segments of s bits.
- 's' can have any value.
- But common value for s = 8.

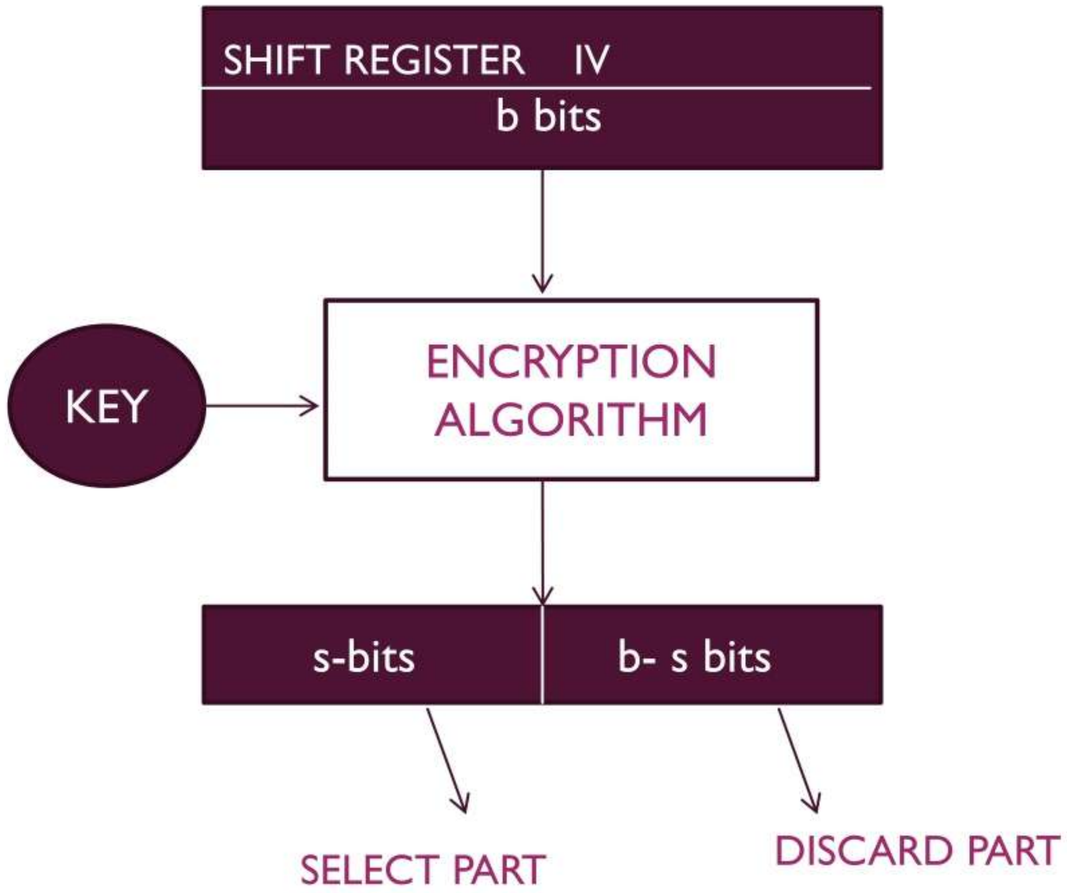
Cipher Feedback (CFB) Mode



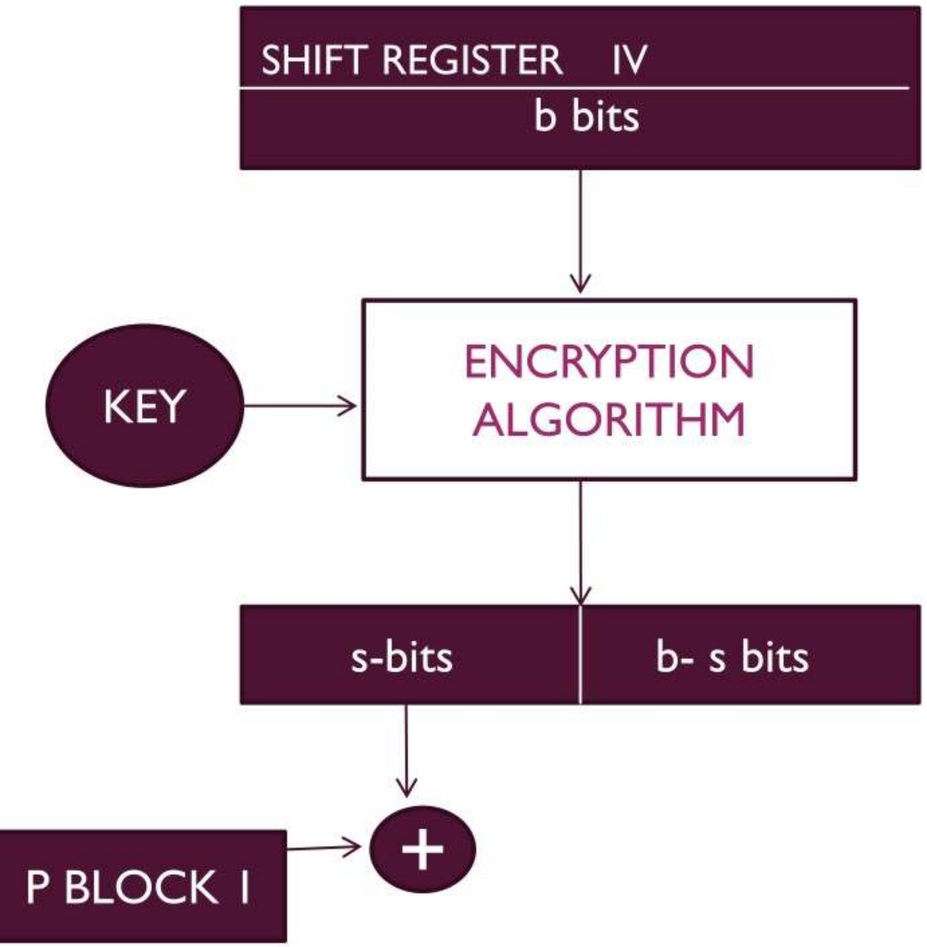
Cipher Feedback (CFB) Mode



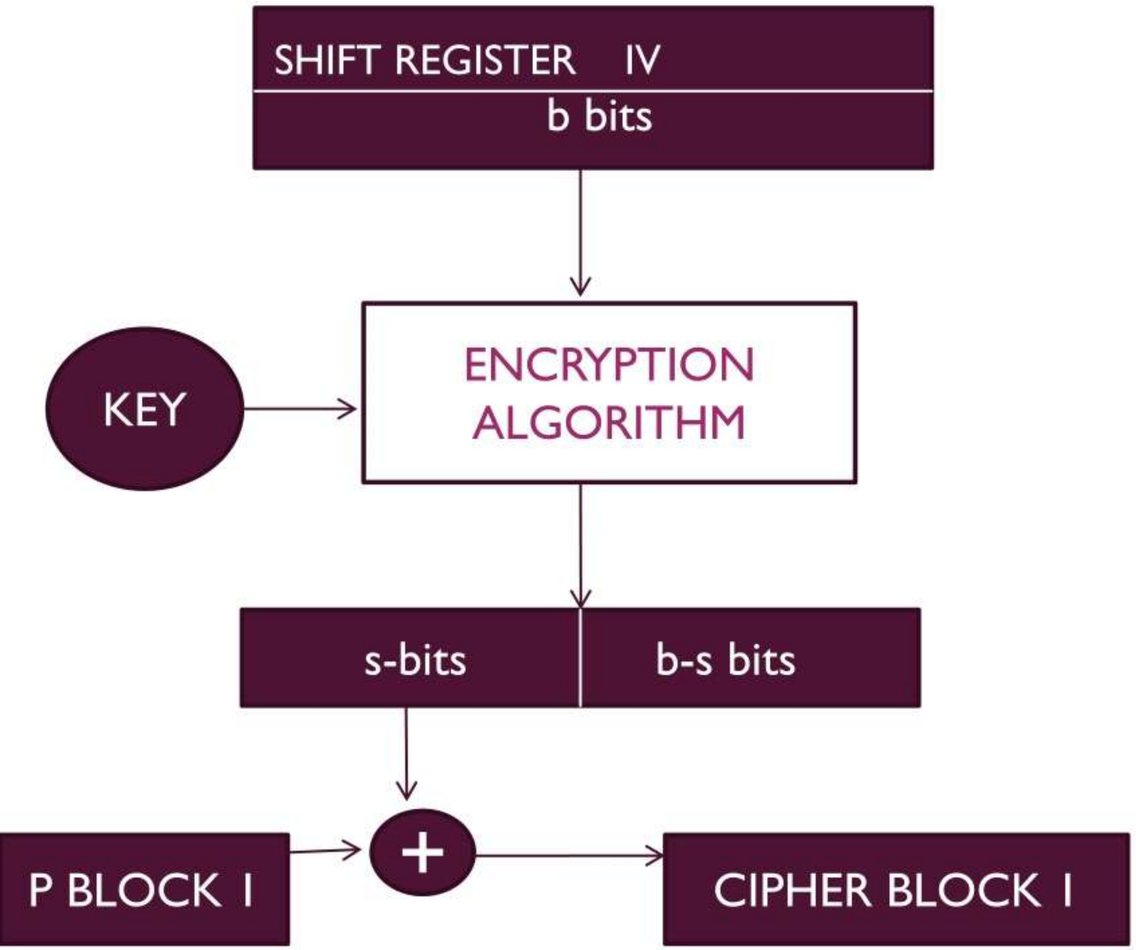
Cipher Feedback (CFB) Mode



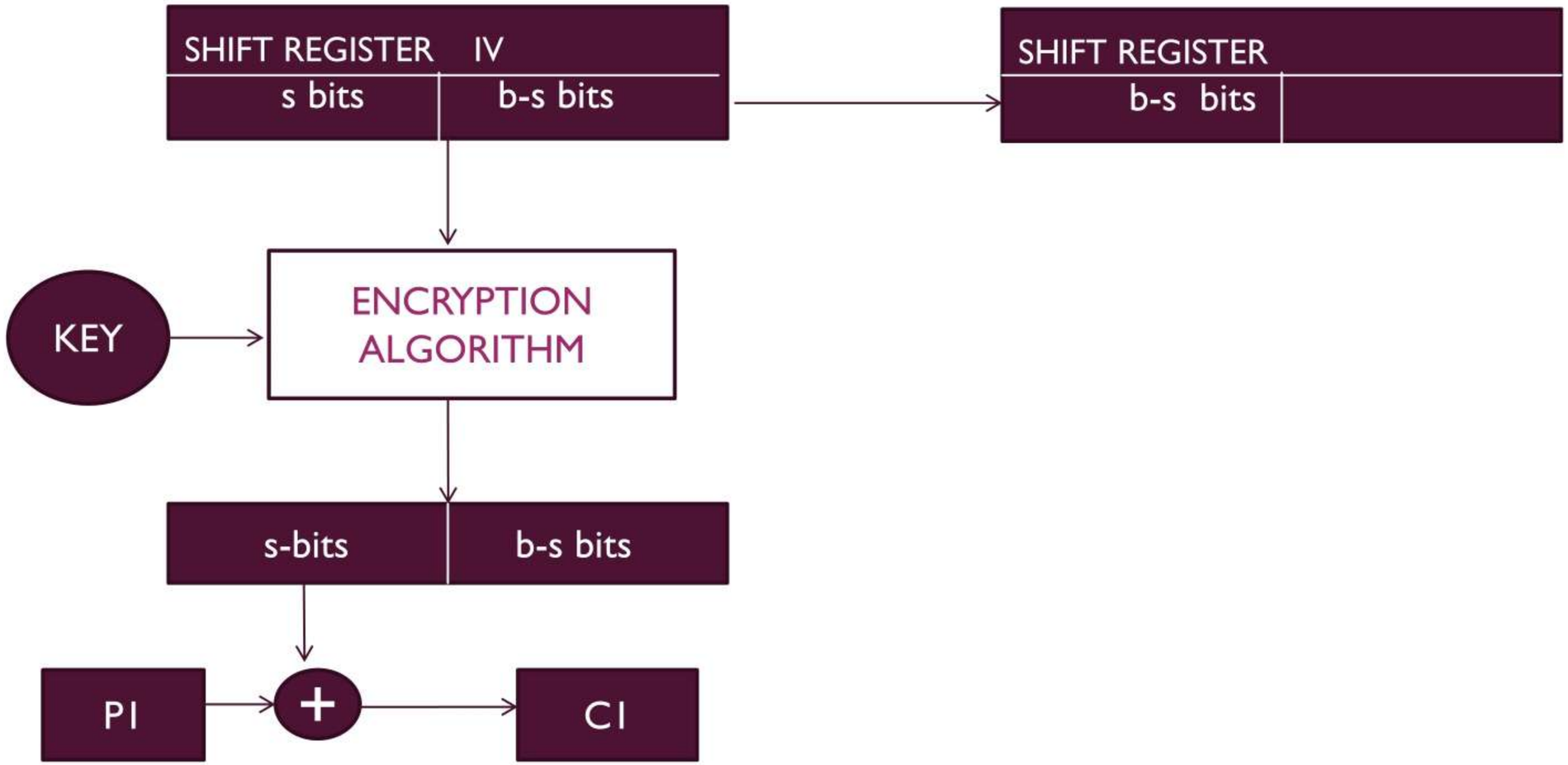
Cipher Feedback (CFB) Mode



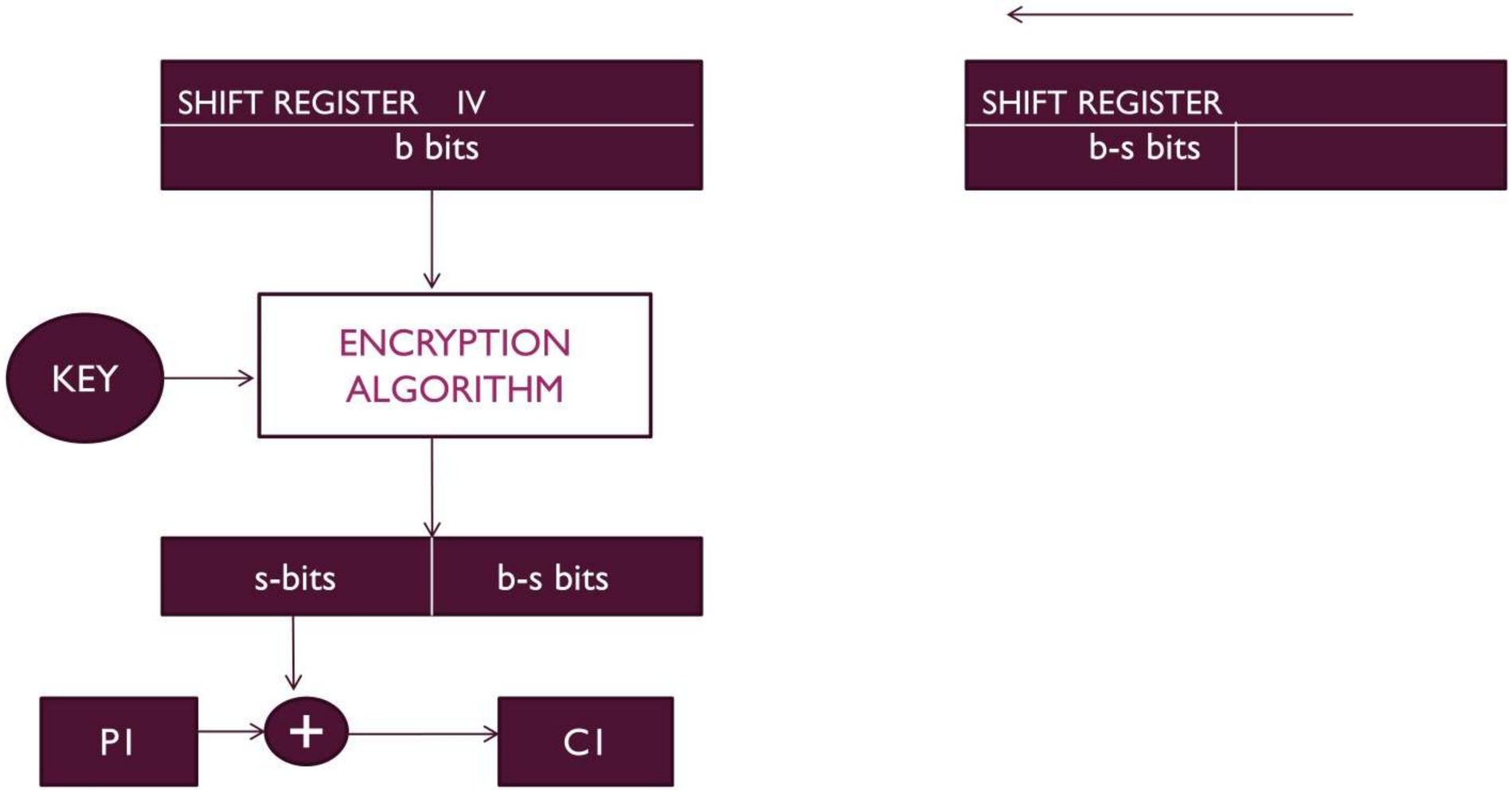
Cipher Feedback (CFB) Mode



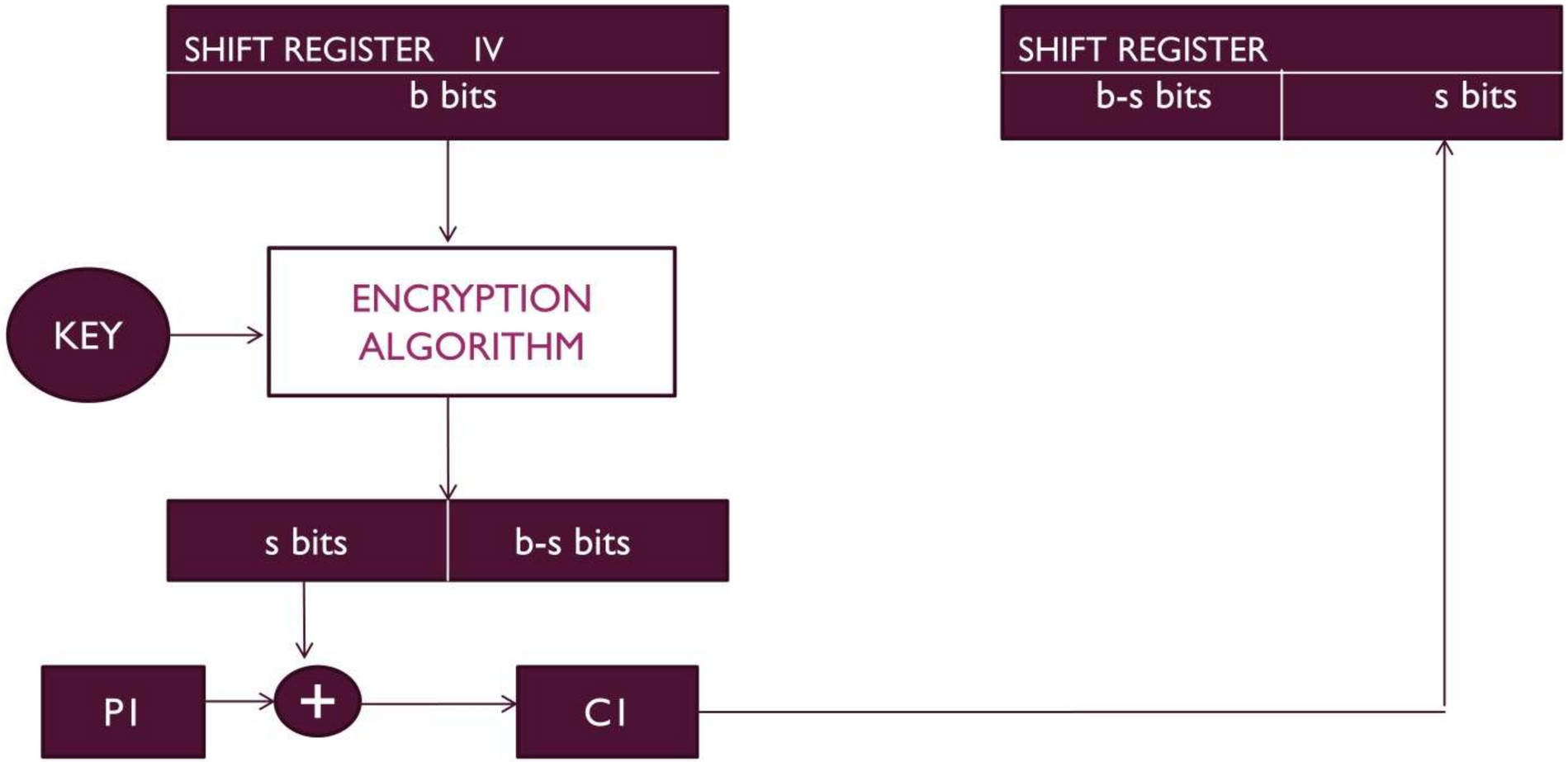
Cipher Feedback (CFB) Mode



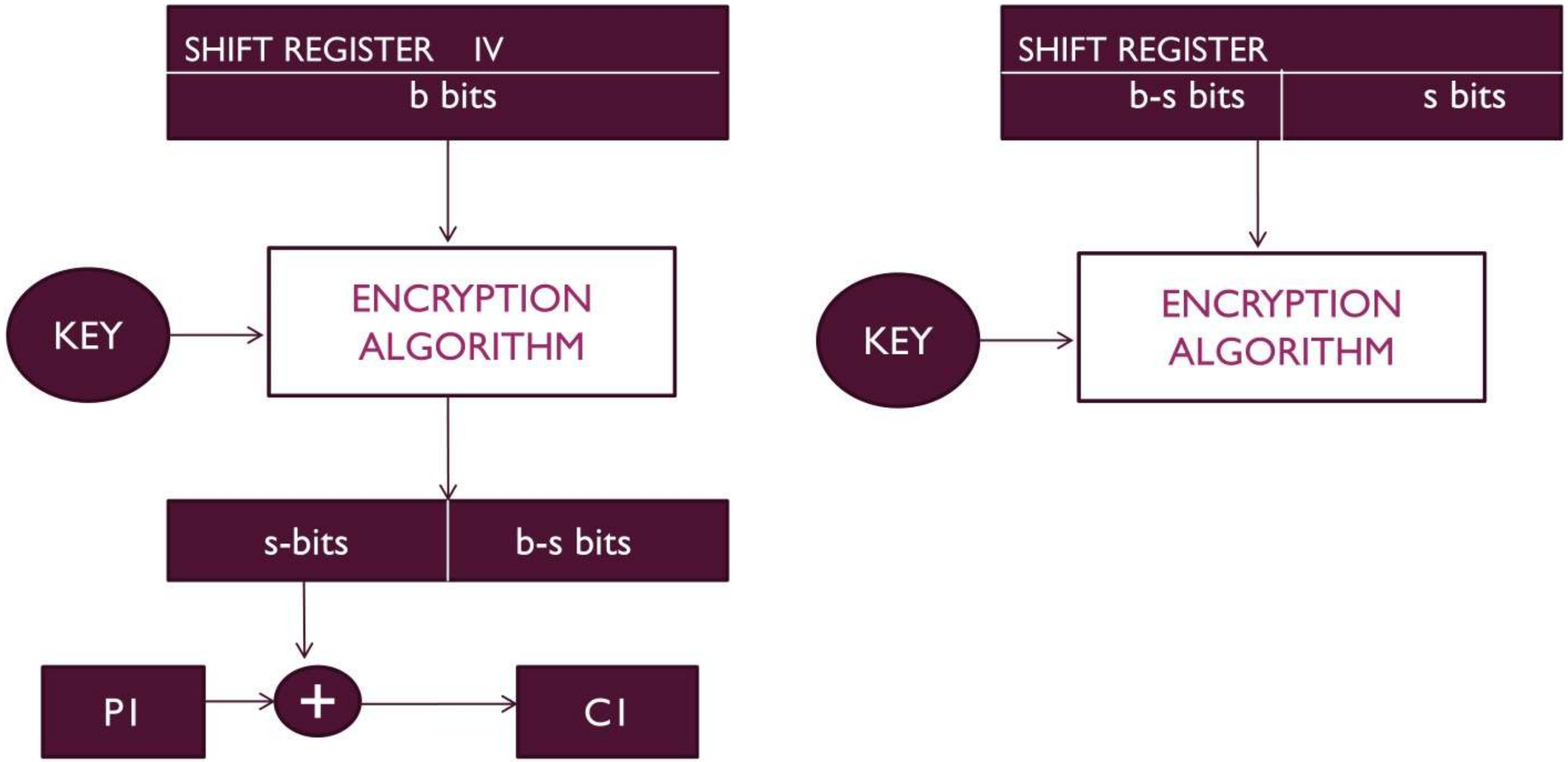
Cipher Feedback (CFB) Mode



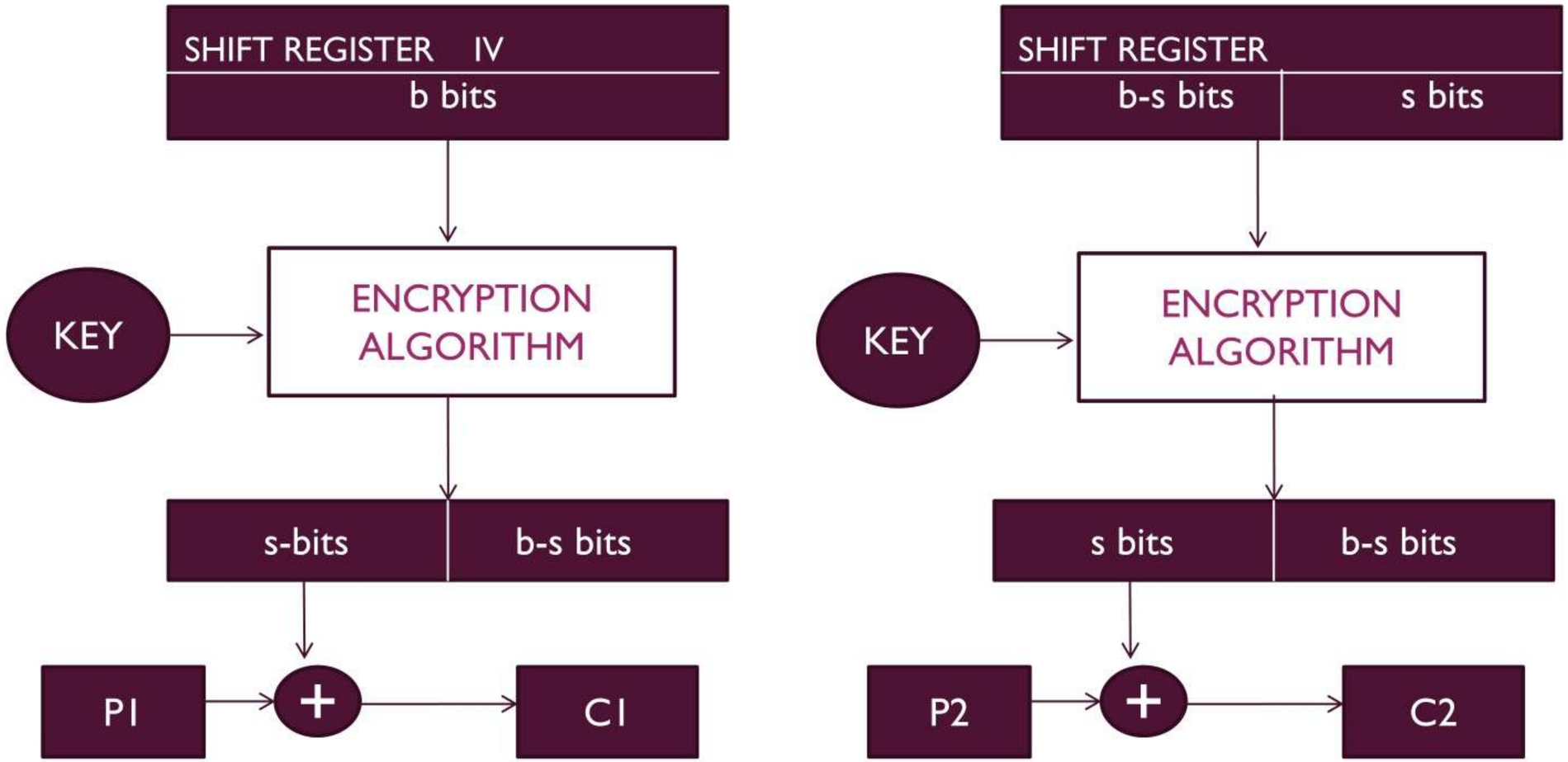
Cipher Feedback (CFB) Mode



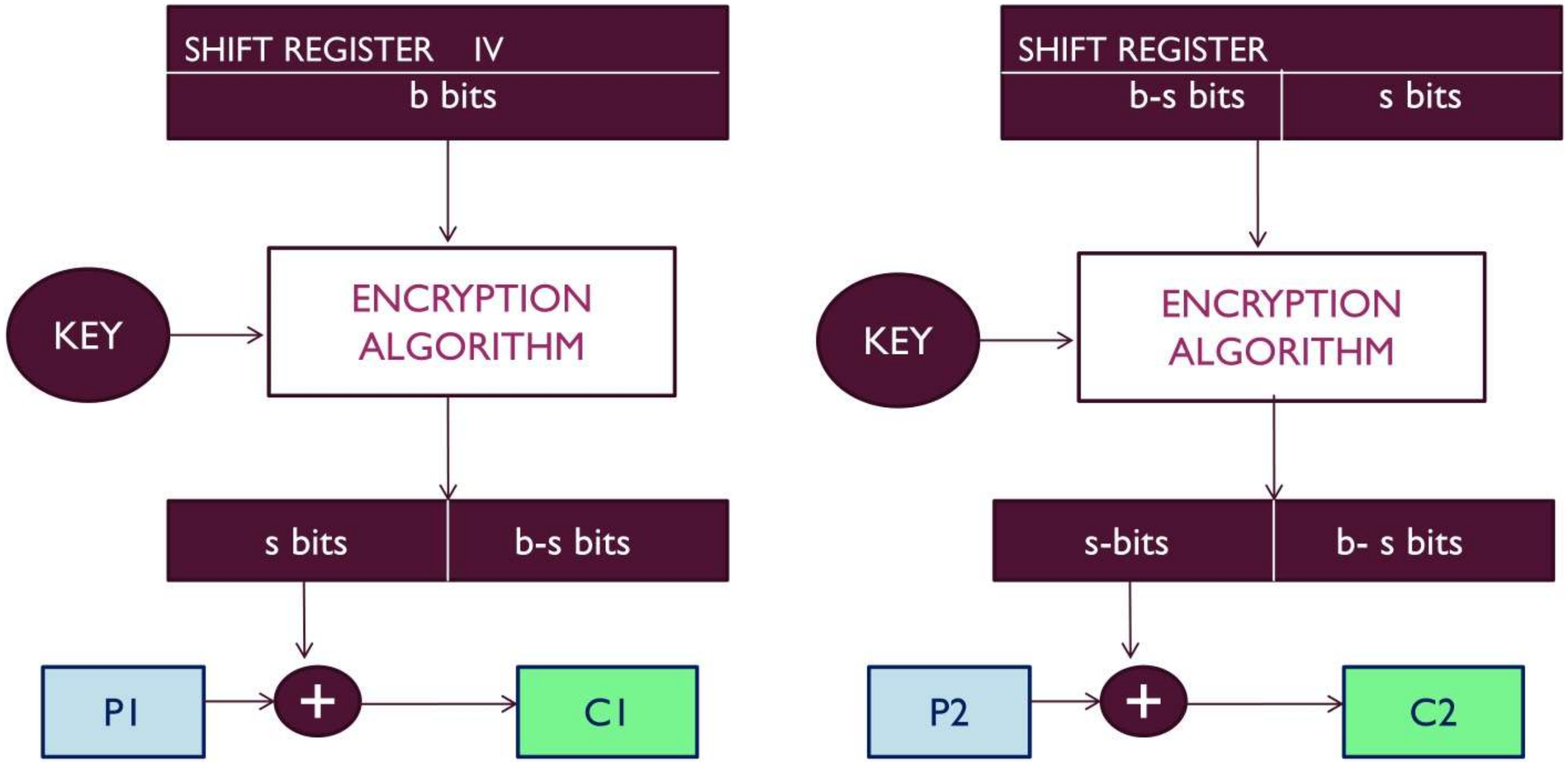
Cipher Feedback (CFB) Mode



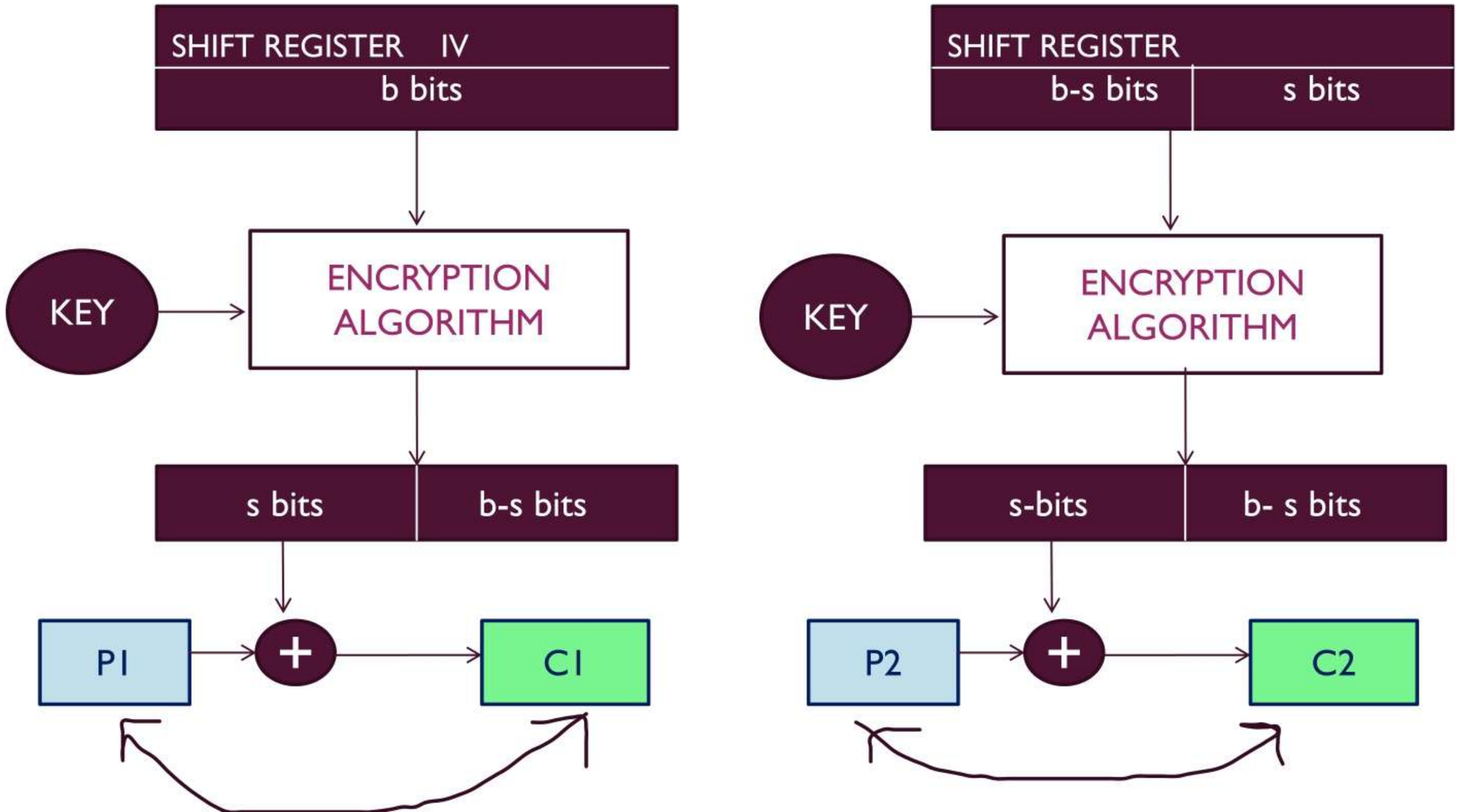
Cipher Feedback (CFB) Mode



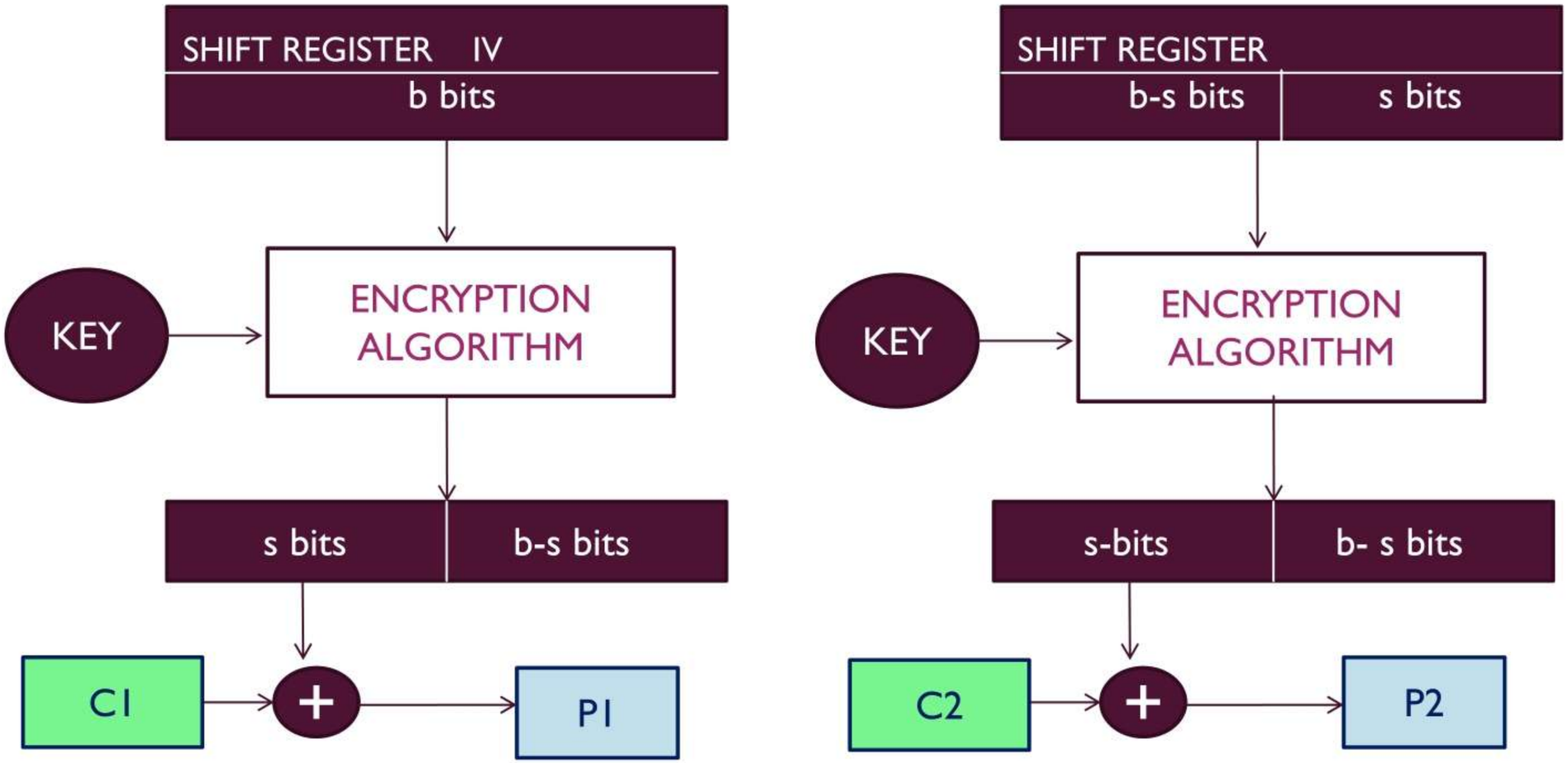
Cipher Feedback (CFB) Mode - Decryption



Cipher Feedback (CFB) Mode - Decryption



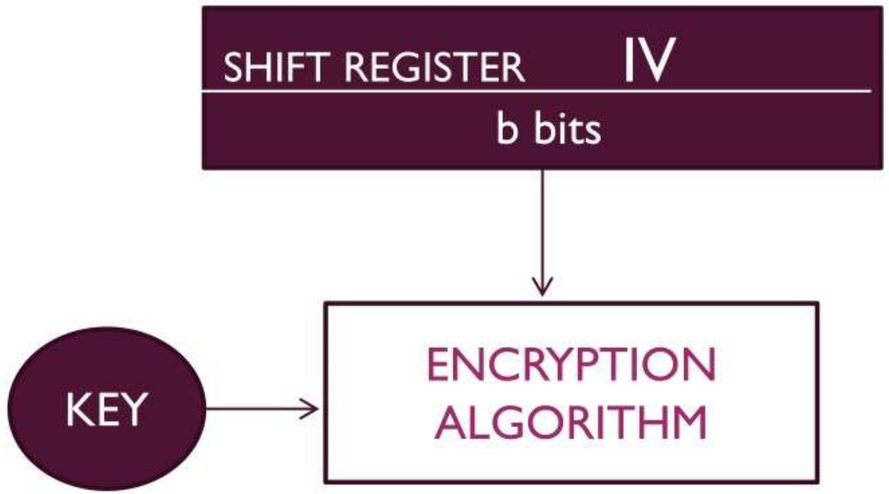
Cipher Feedback (CFB) Mode - Decryption



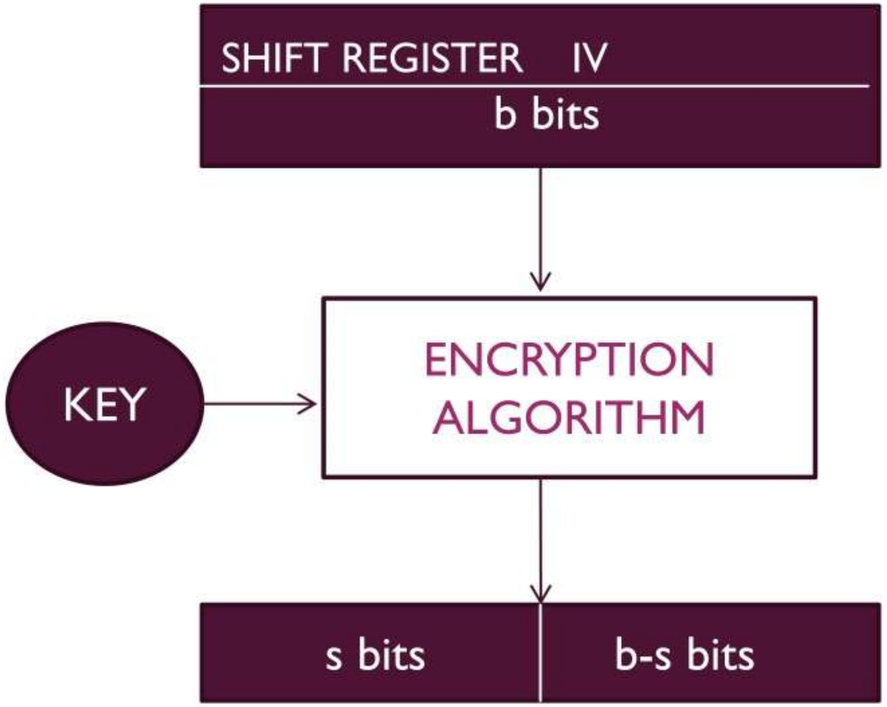
Output Feedback (OFB) Mode

- The output feedback (OFB) mode is similar in structure to that of CFB.
- The output of the encryption function that is fed back to the shift register in OFB, whereas in CFB the ciphertext unit is fed back to the shift register.

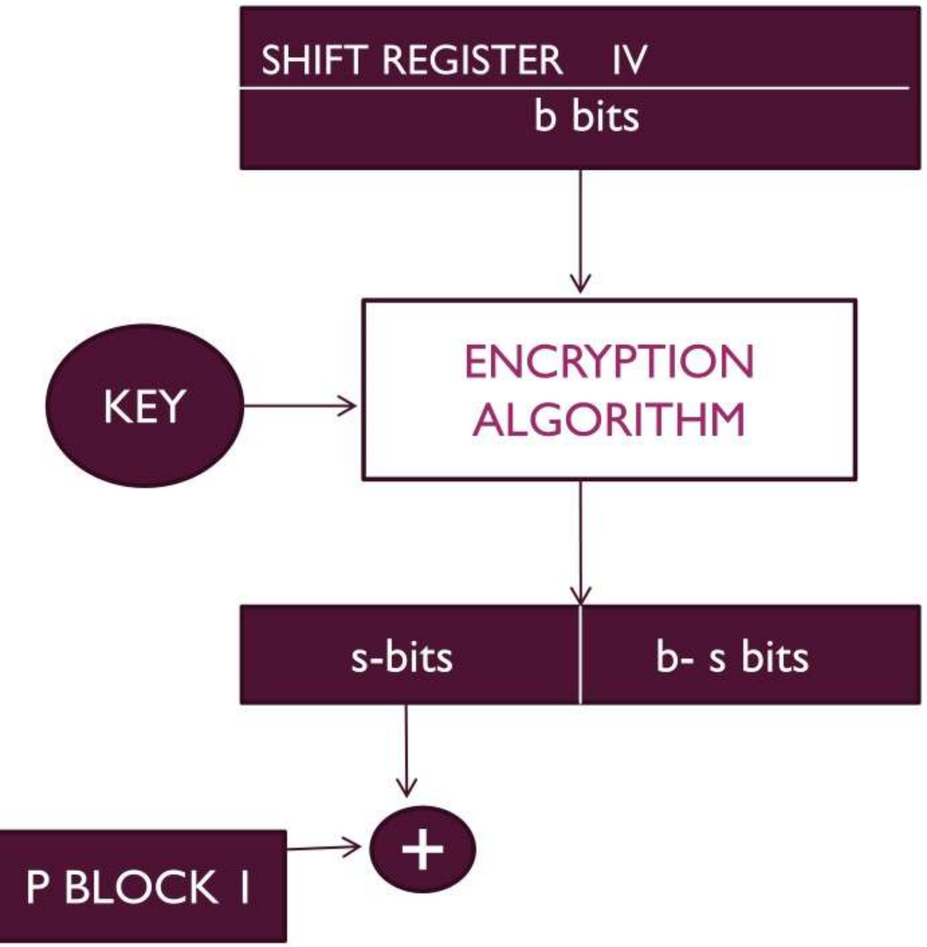
Output Feedback (OFB) Mode



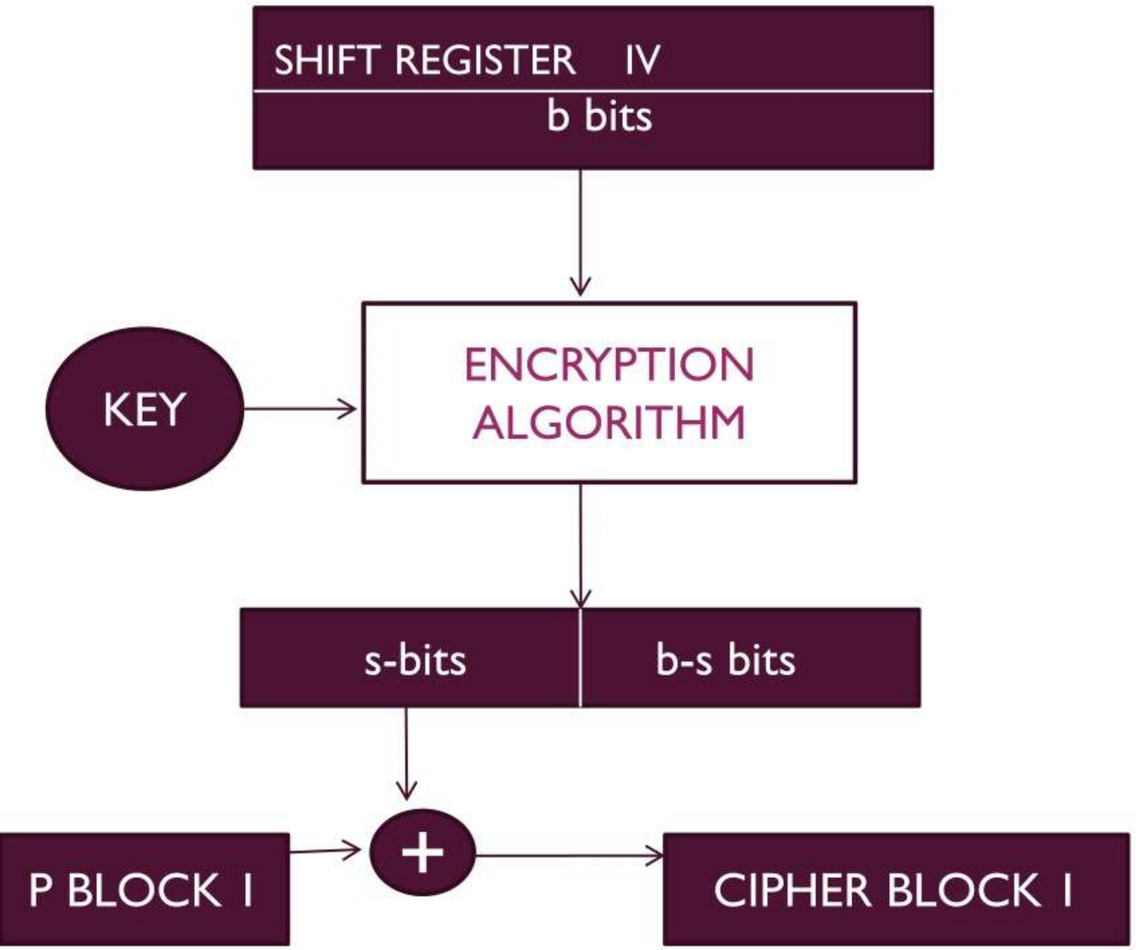
Output Feedback (OFB) Mode



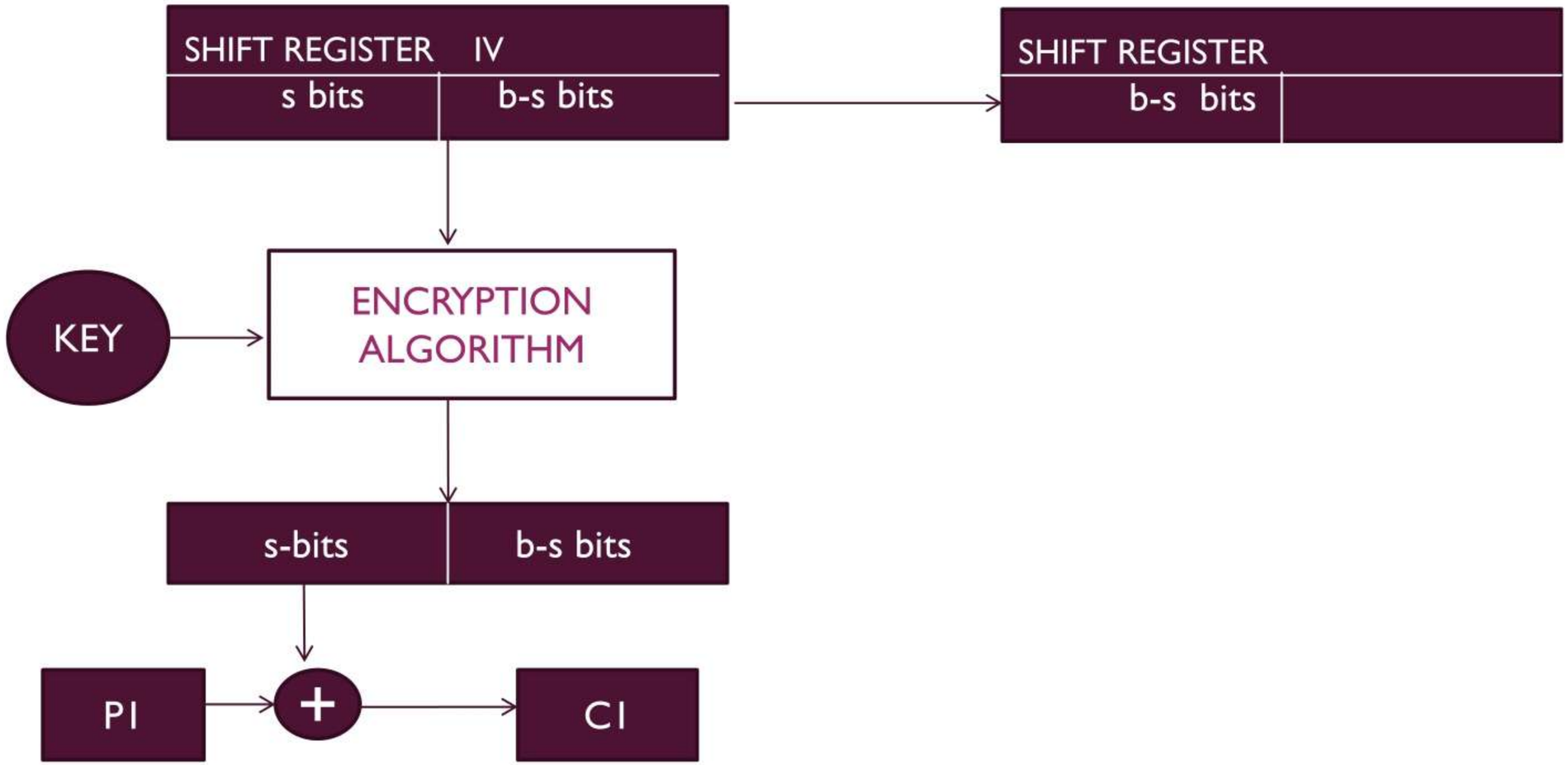
Output Feedback (OFB) Mode



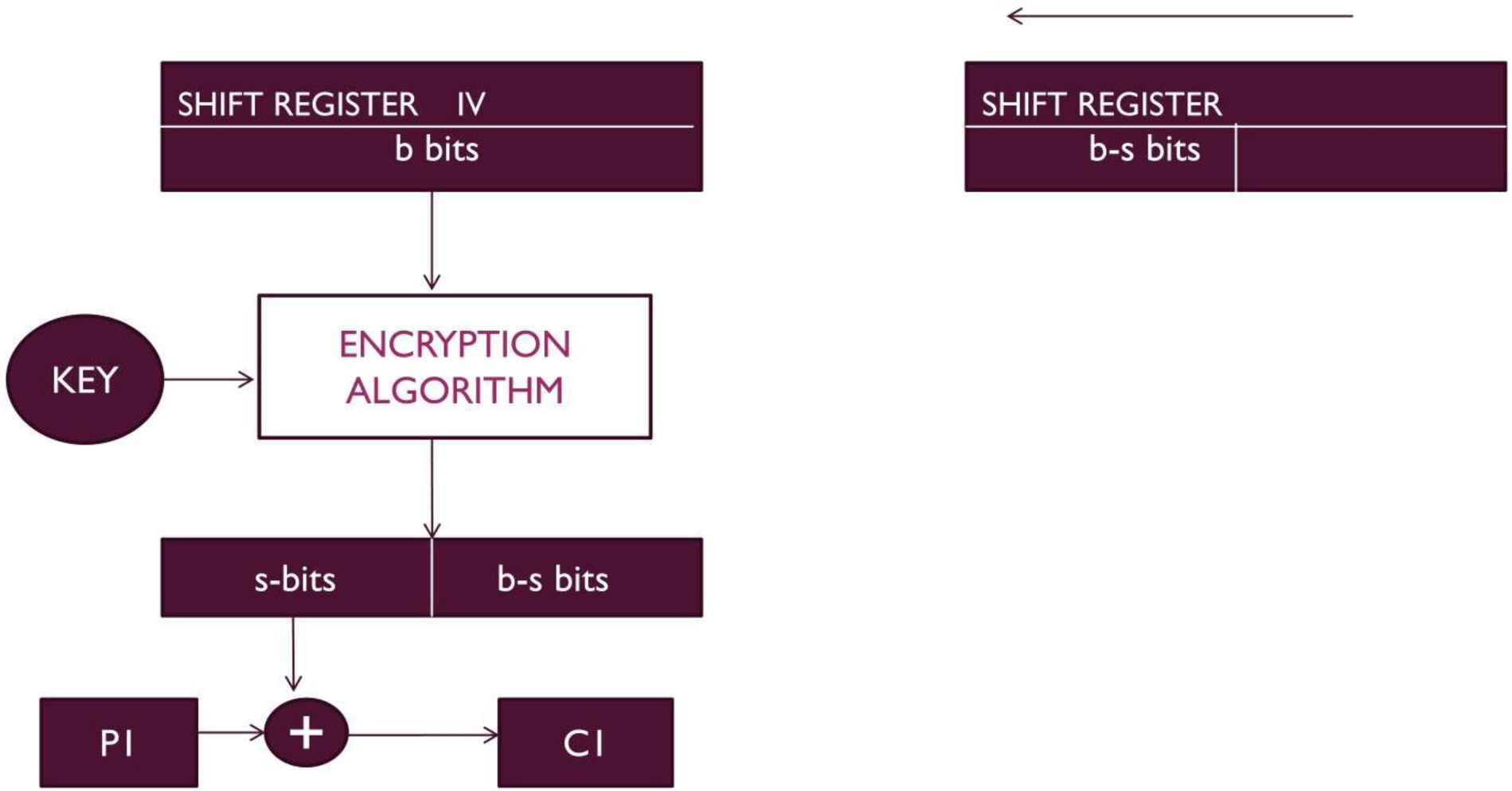
Output Feedback (OFB) Mode



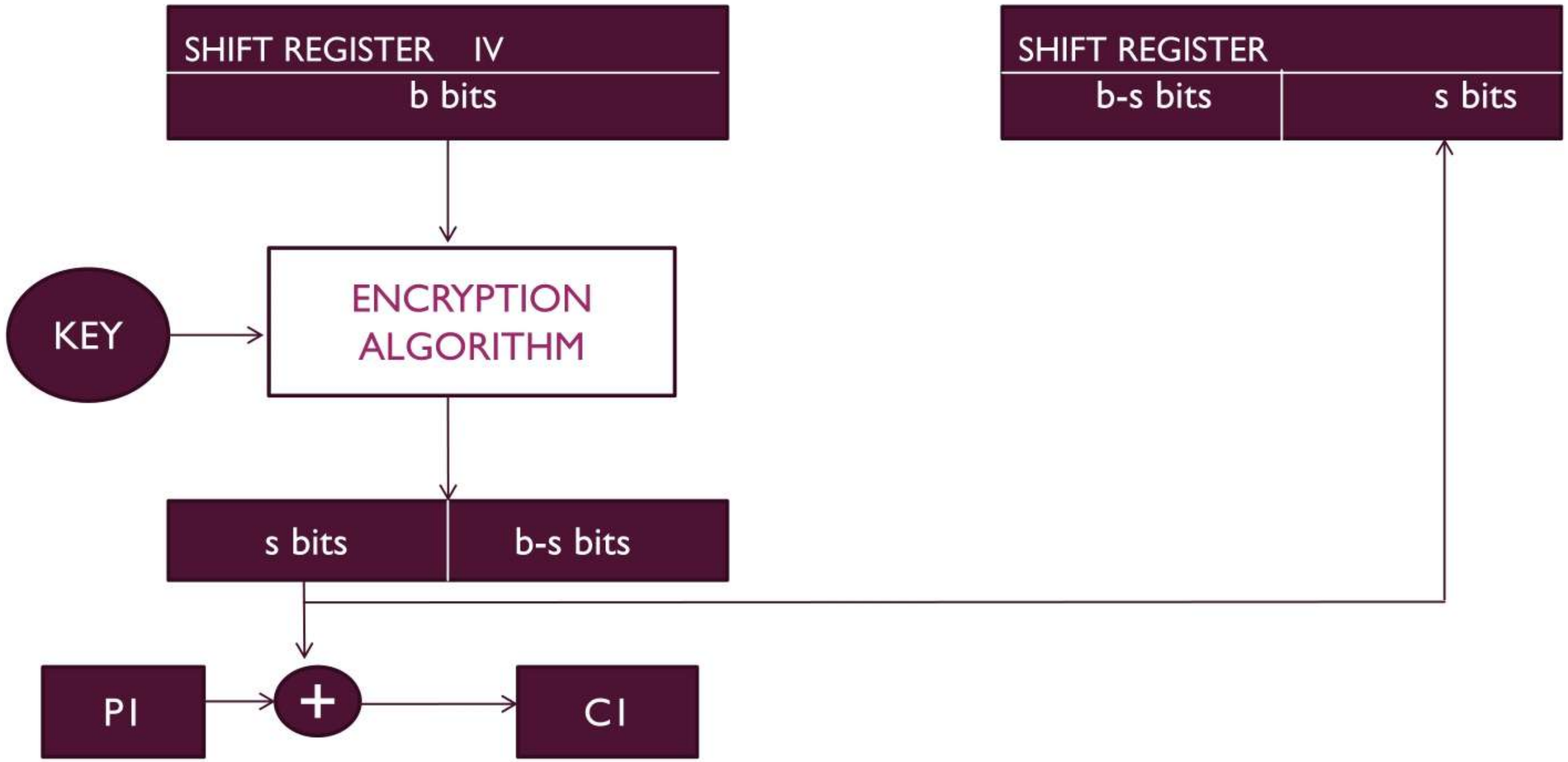
Output Feedback (OFB) Mode



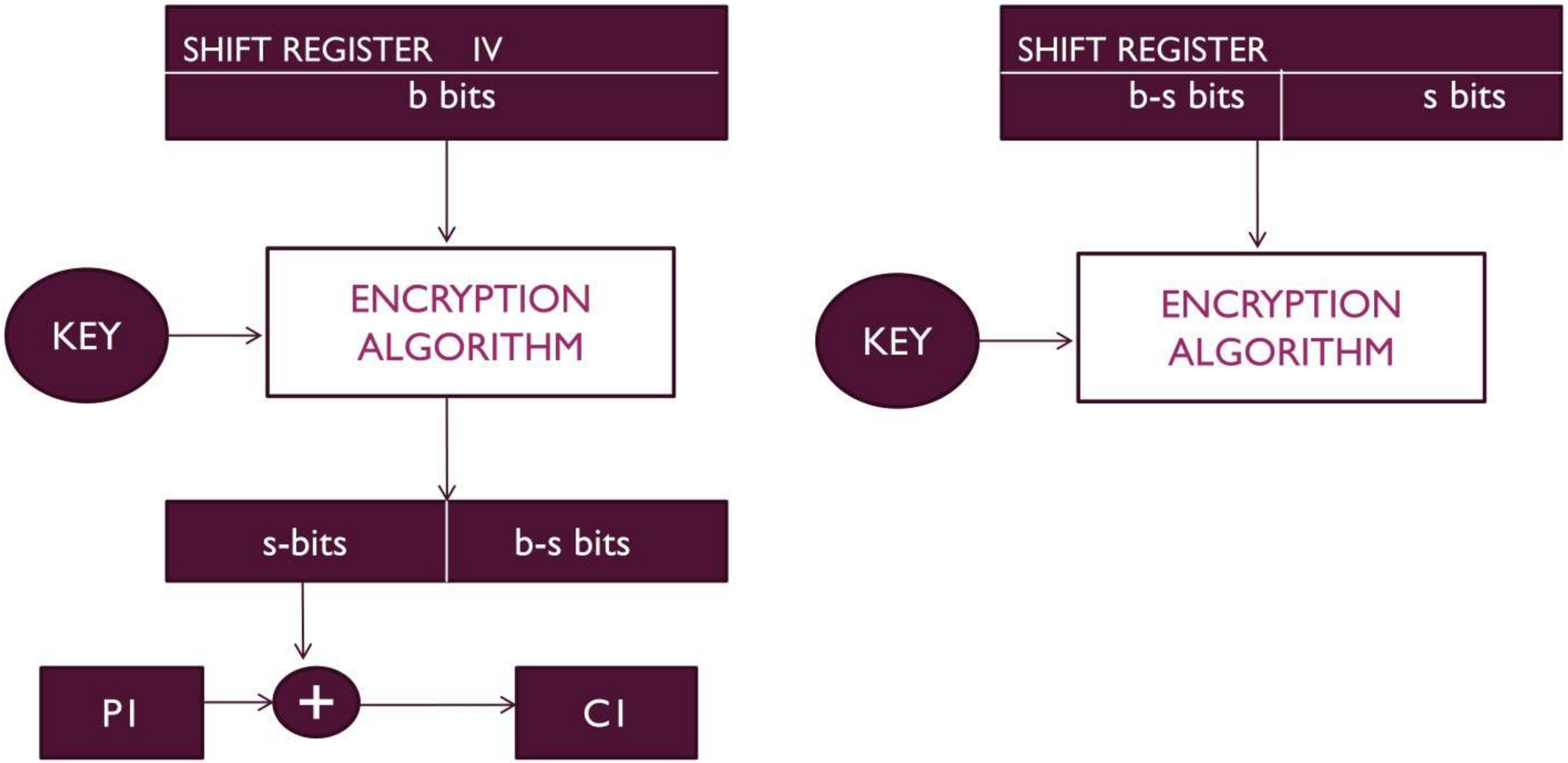
Output Feedback (OFB) Mode



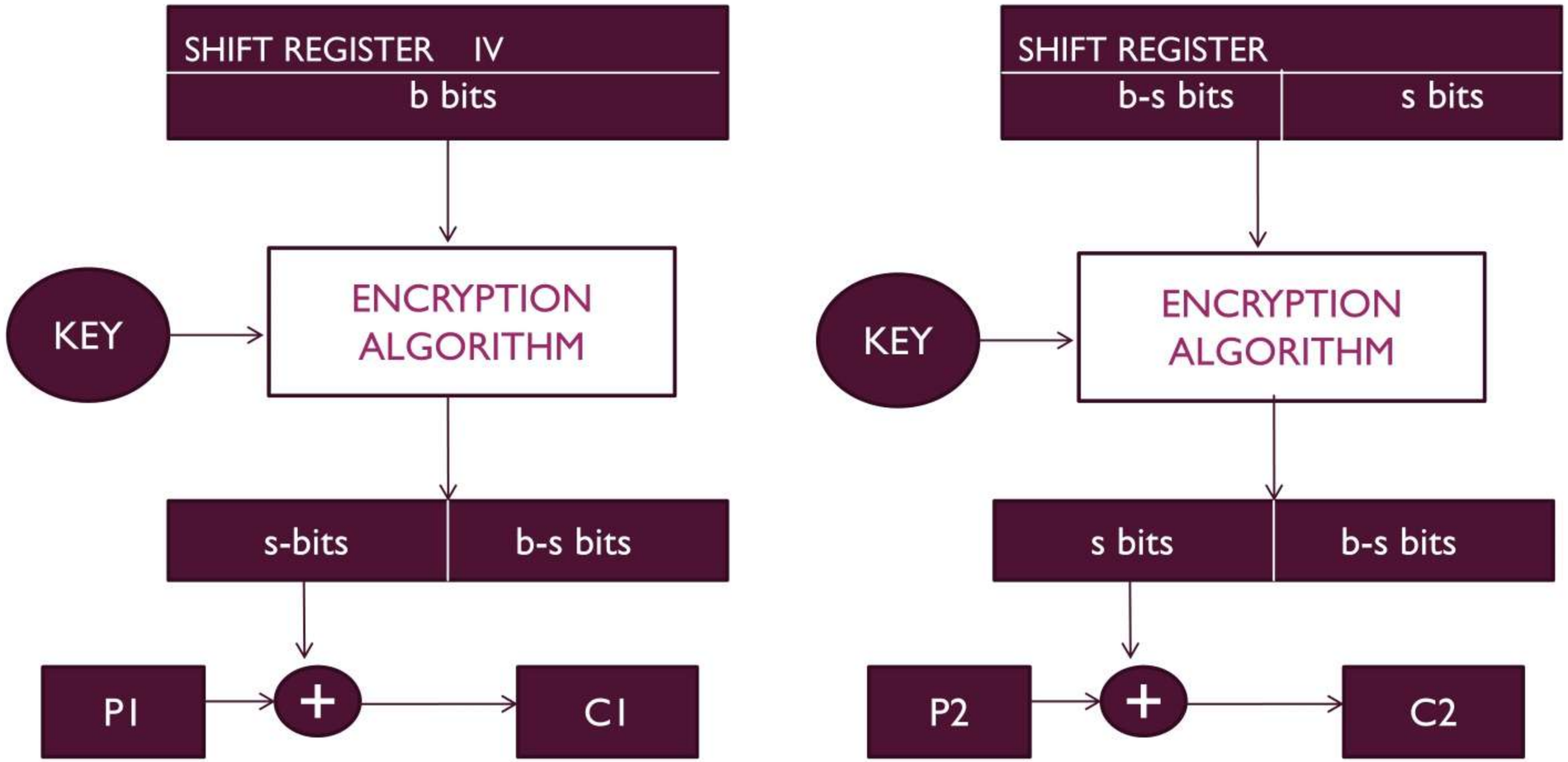
Output Feedback (OFB) Mode



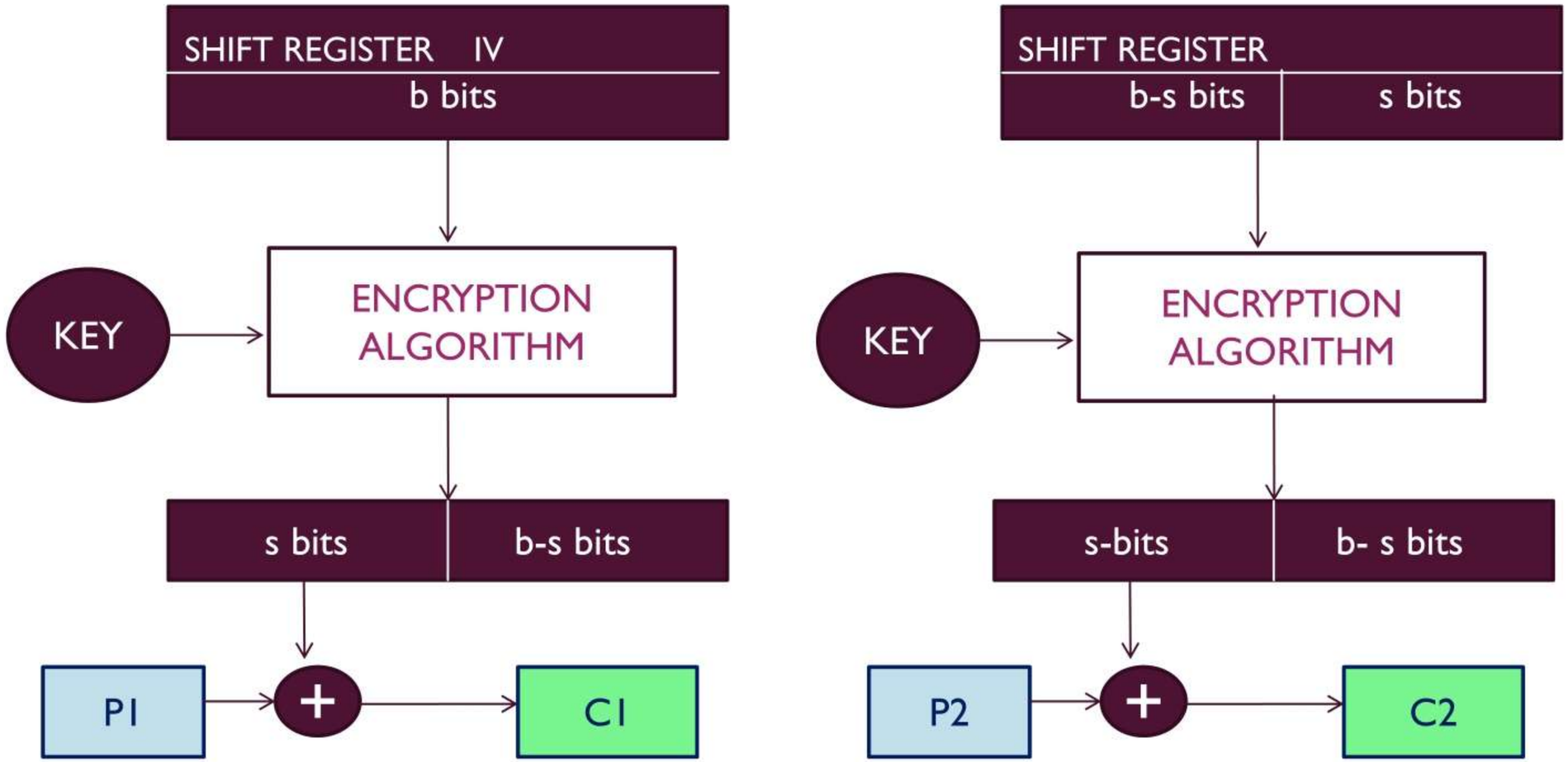
Output Feedback (OFB) Mode



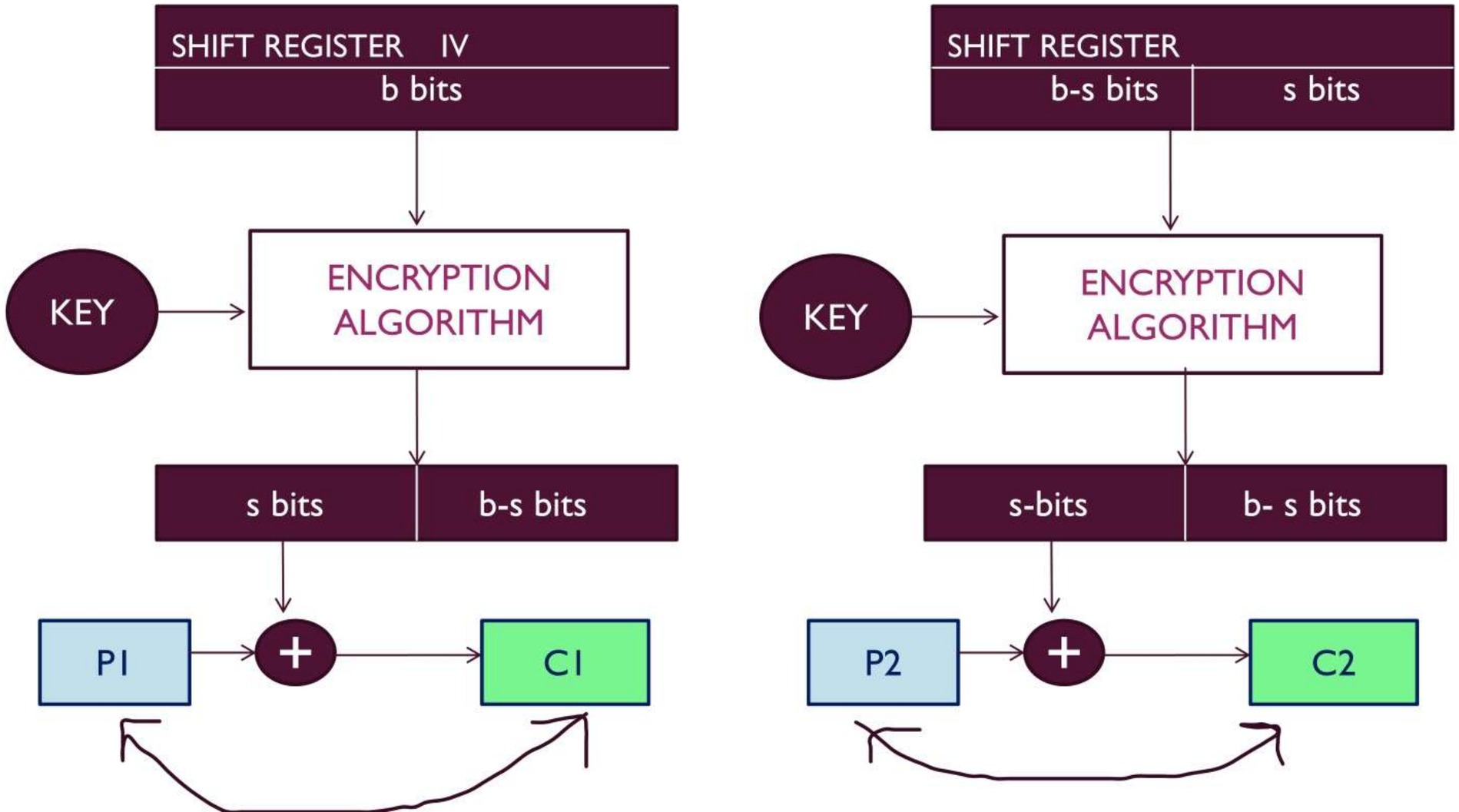
Output Feedback (OFB) Mode



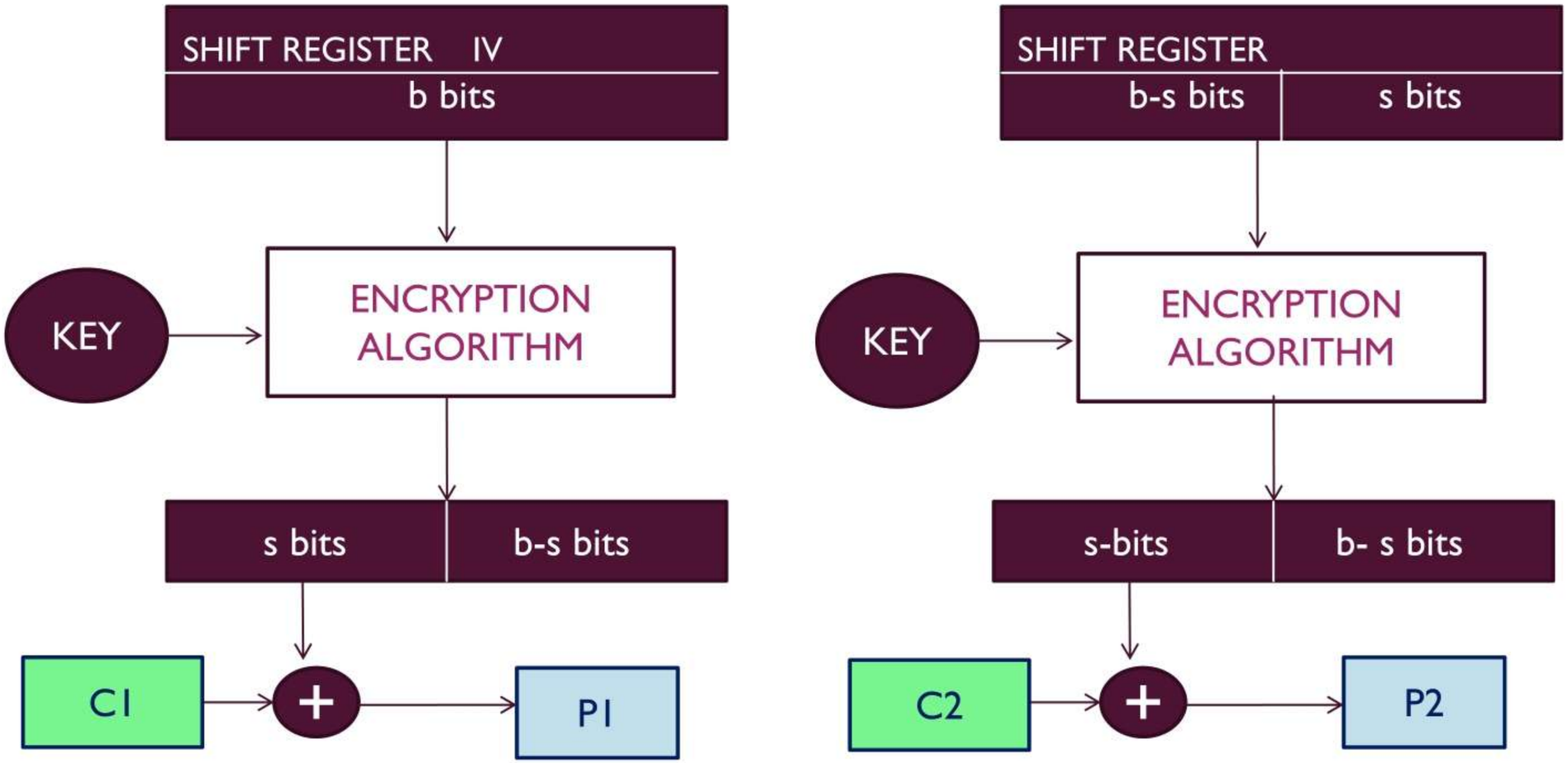
Cipher Feedback (CFB) Mode - Decryption



Cipher Feedback (CFB) Mode - Decryption



Cipher Feedback (CFB) Mode - Decryption

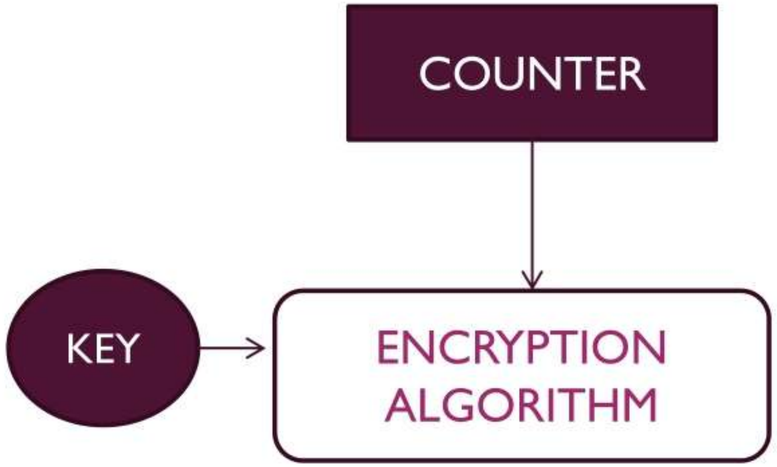


Counter (CTR) Mode

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.

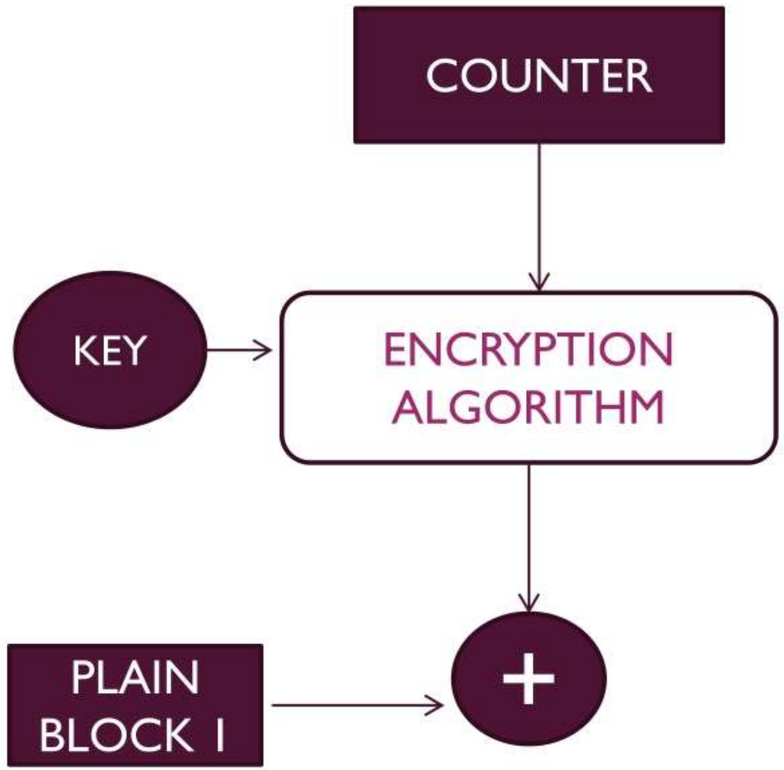
Counter (CTR) Mode

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



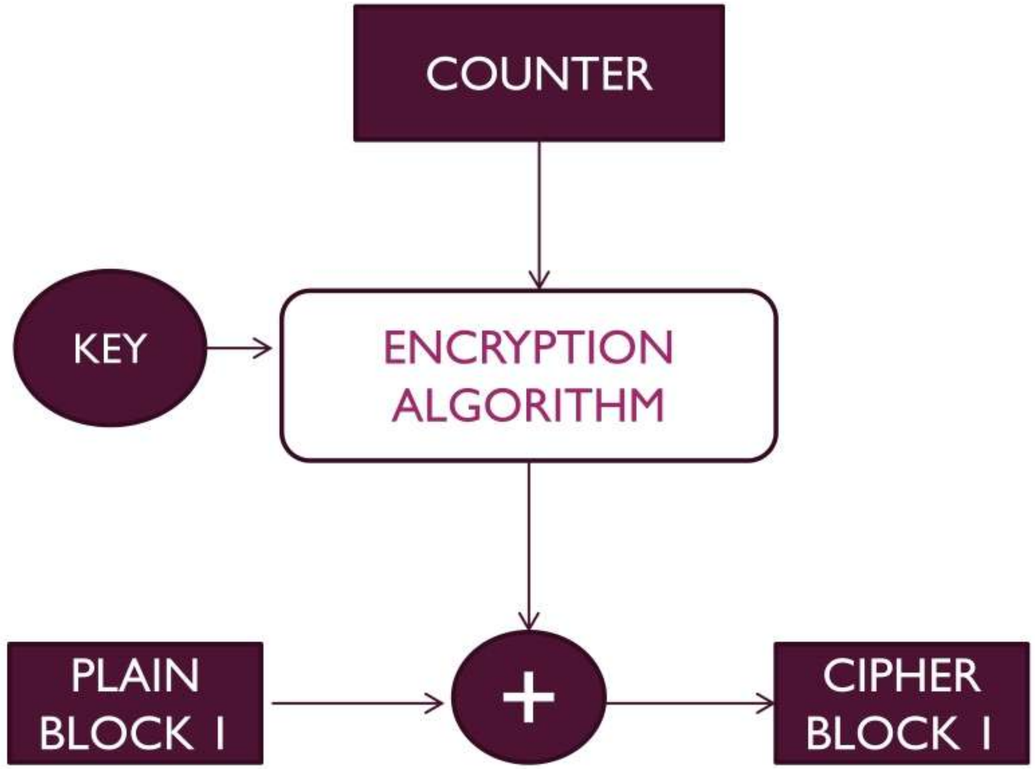
Counter (CTR) Mode

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



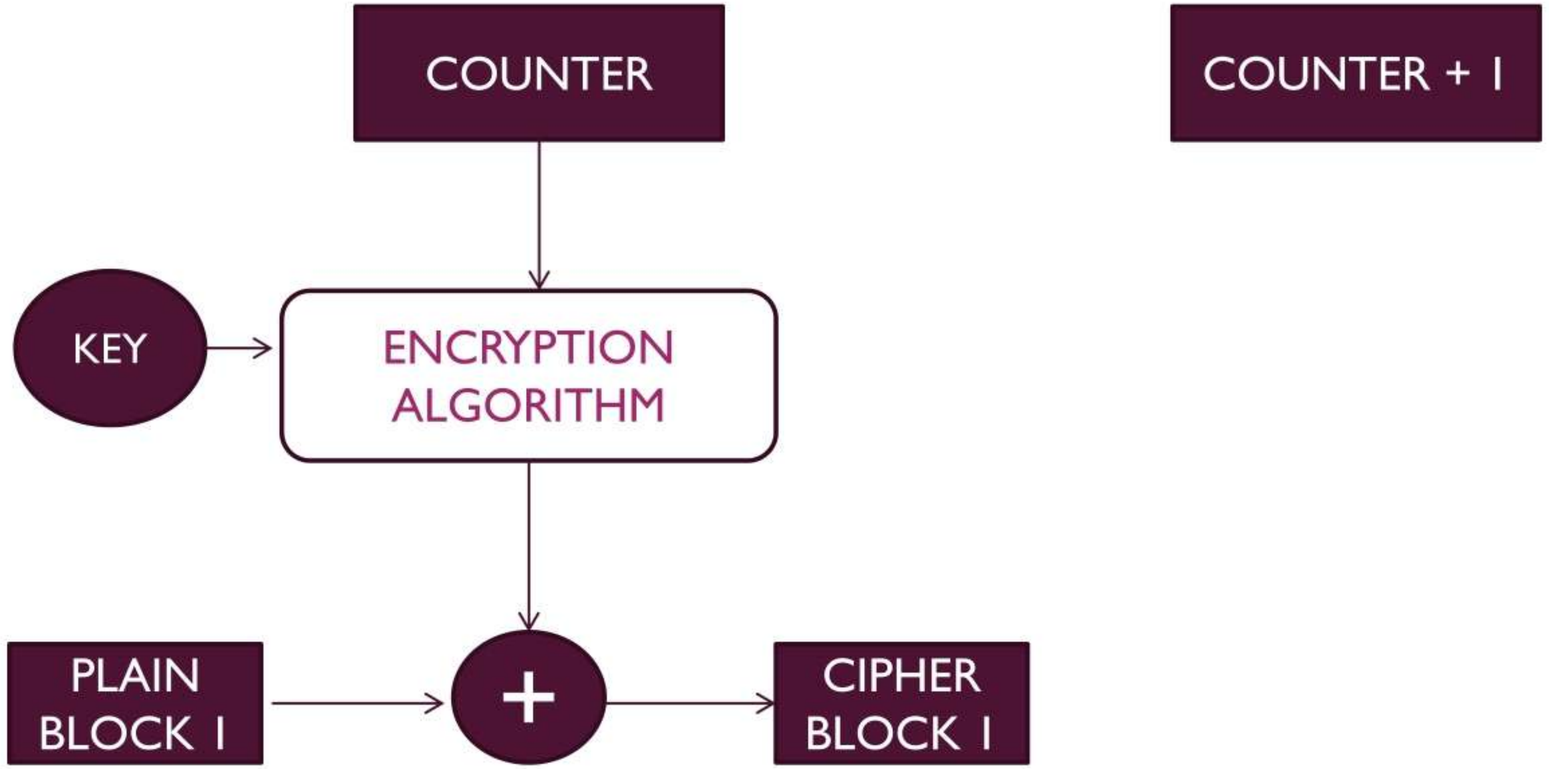
Counter (CTR) Mode

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



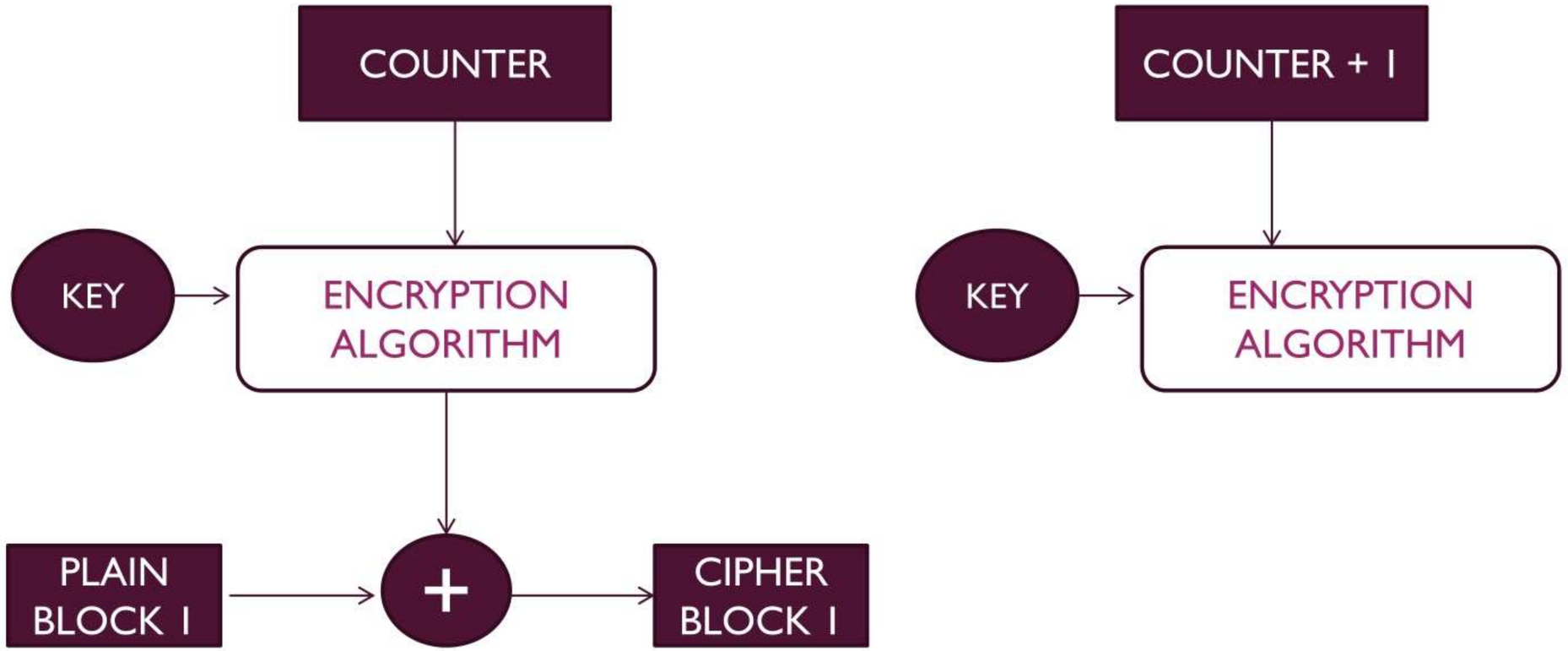
Counter (CTR) Mode

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



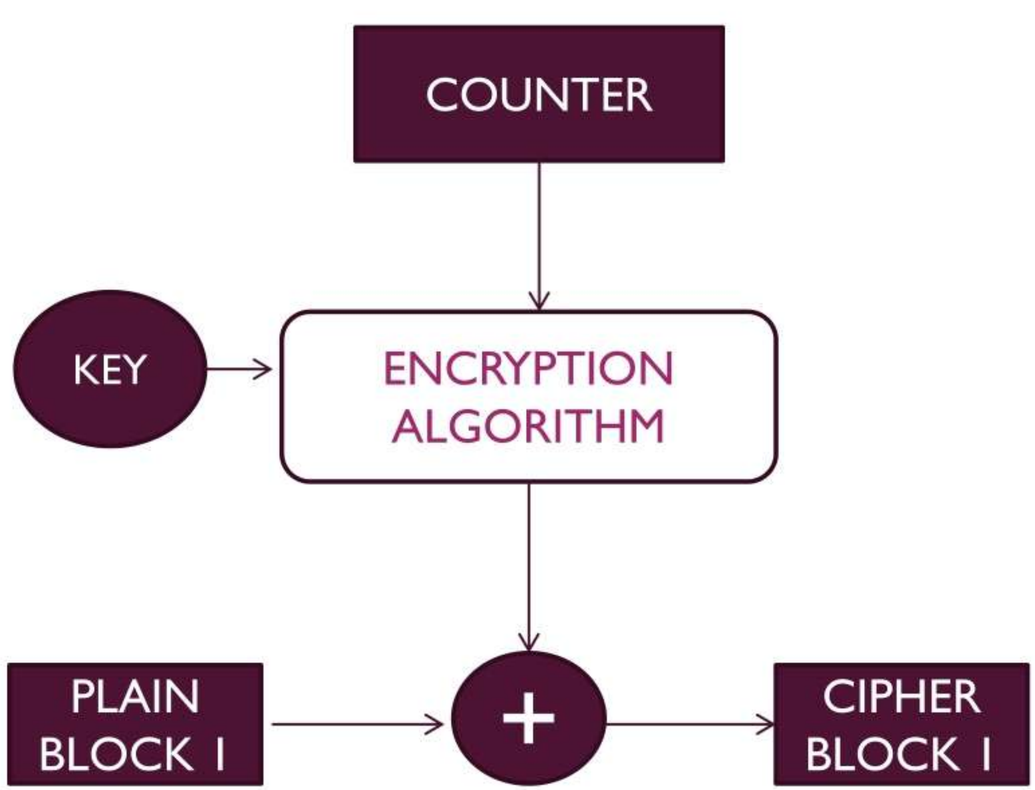
Counter (CTR) Mode

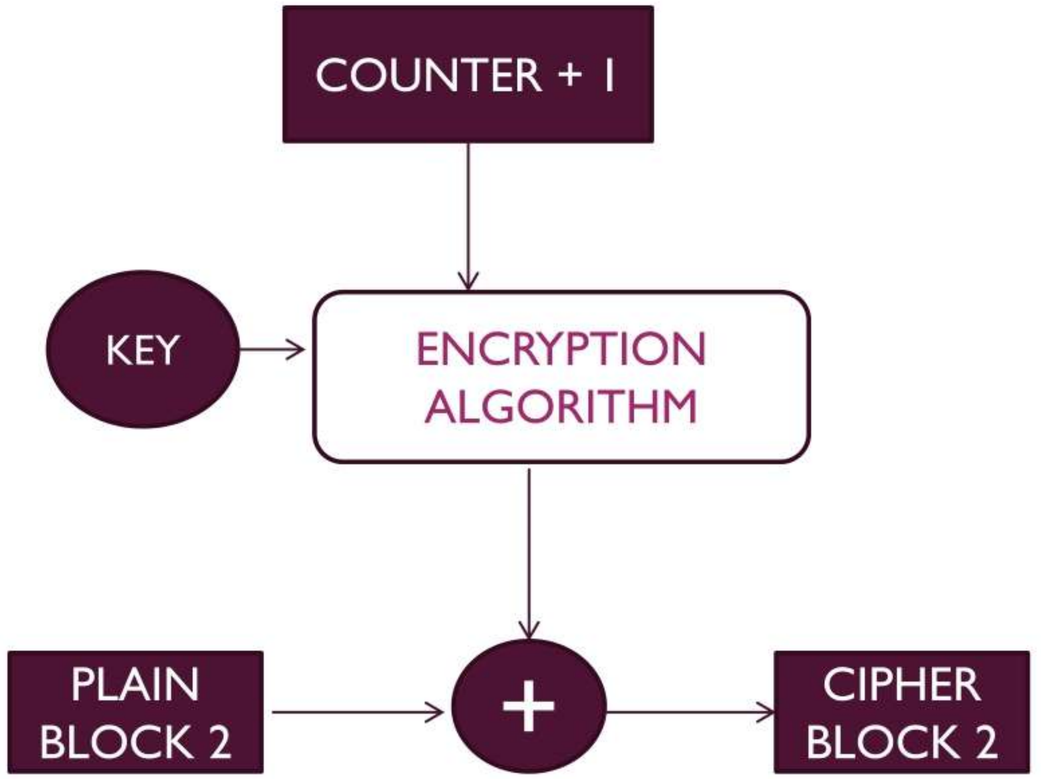
- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



Counter (CTR) Mode

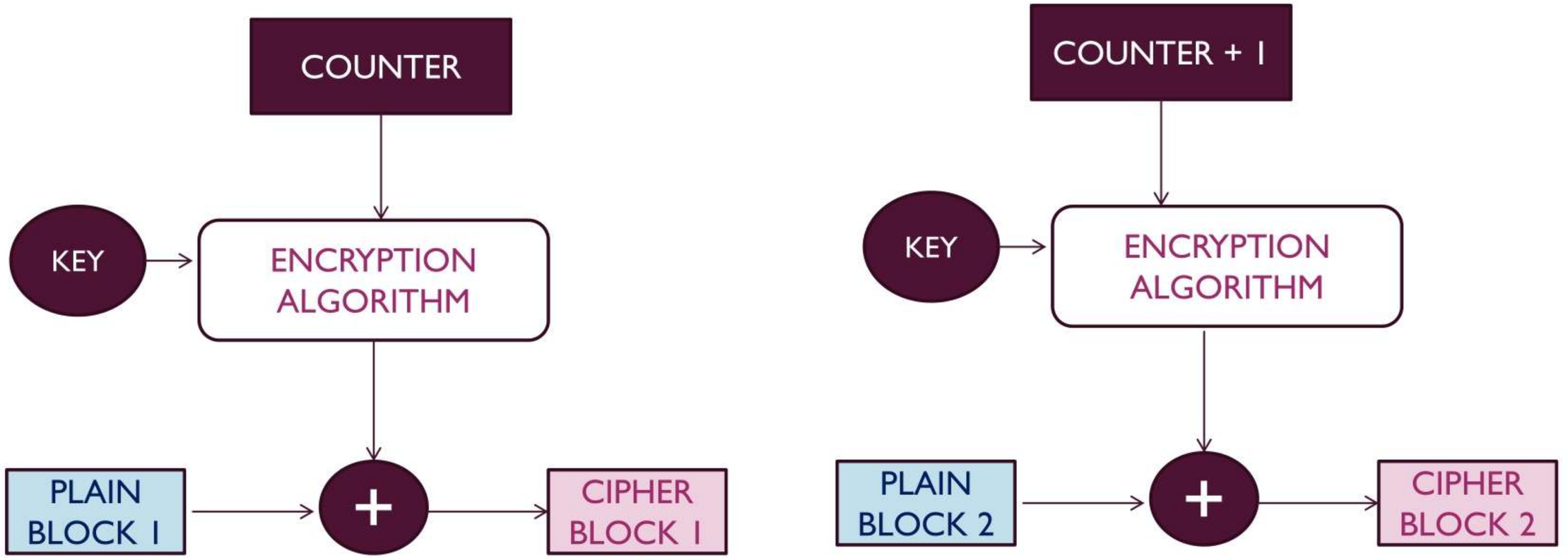
- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.





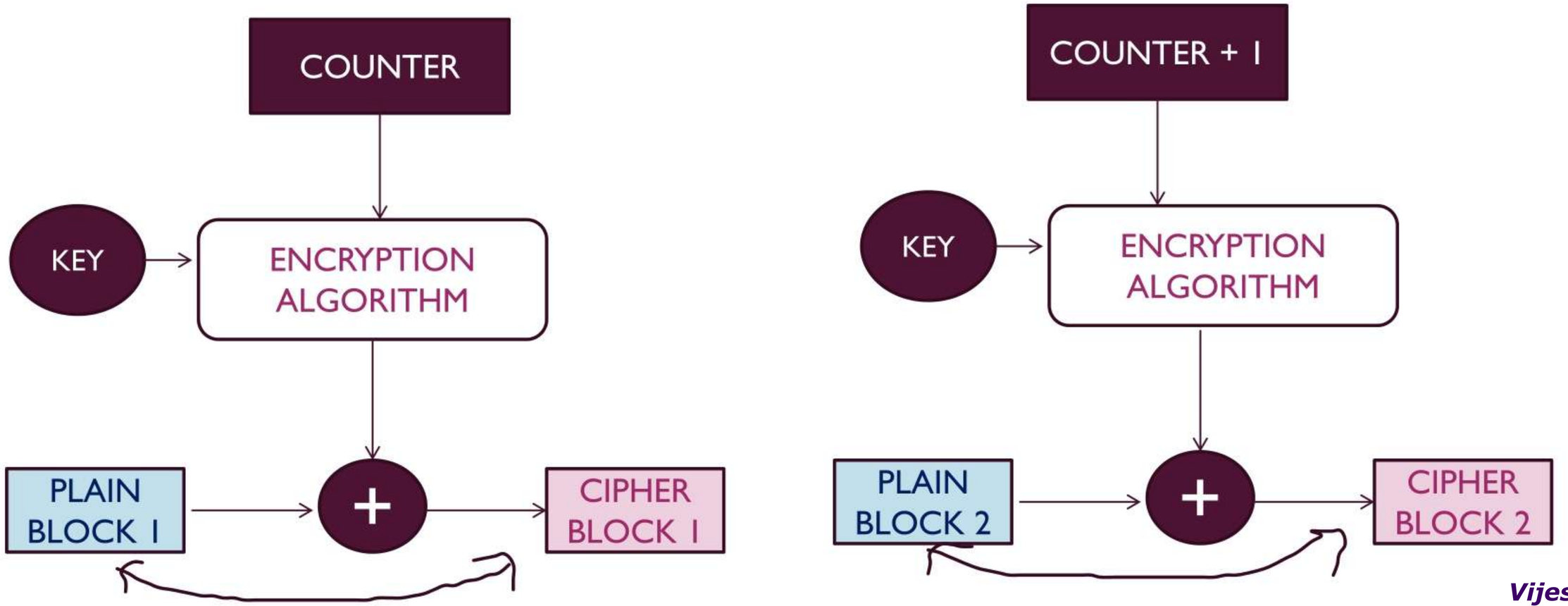
Counter (CTR) Mode - Decryption

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



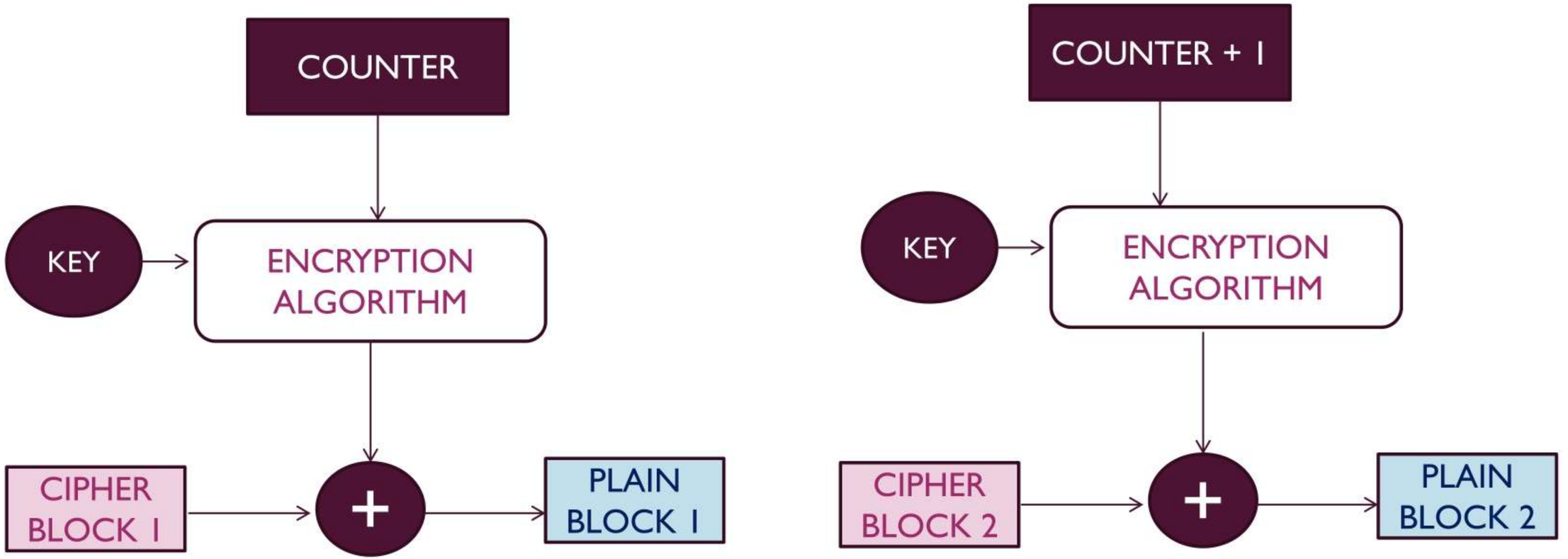
Counter (CTR) Mode - Decryption

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



Counter (CTR) Mode - Decryption

- A counter, equal to the plaintext block size is used.
- The counter is initialized to some value and then incremented by 1 for each subsequent block.



Counter (CTR) Mode

- Simple and fast.
- There is no chaining.
- Counter value need not be shared.
- But both parties need to synchronize the counter.

THANK YOU

Vijesh Nair