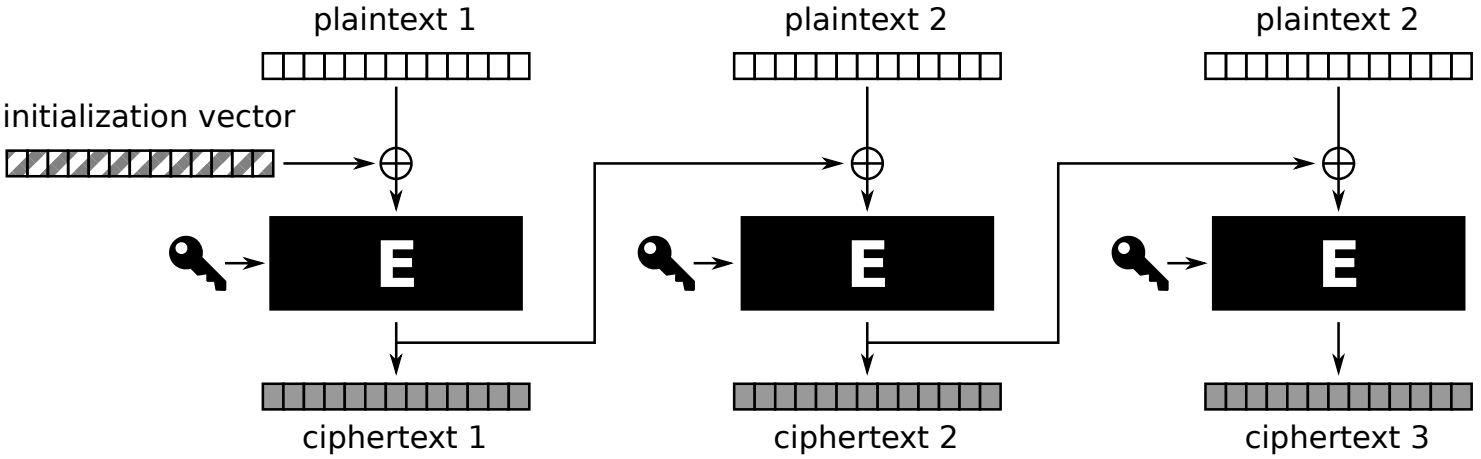
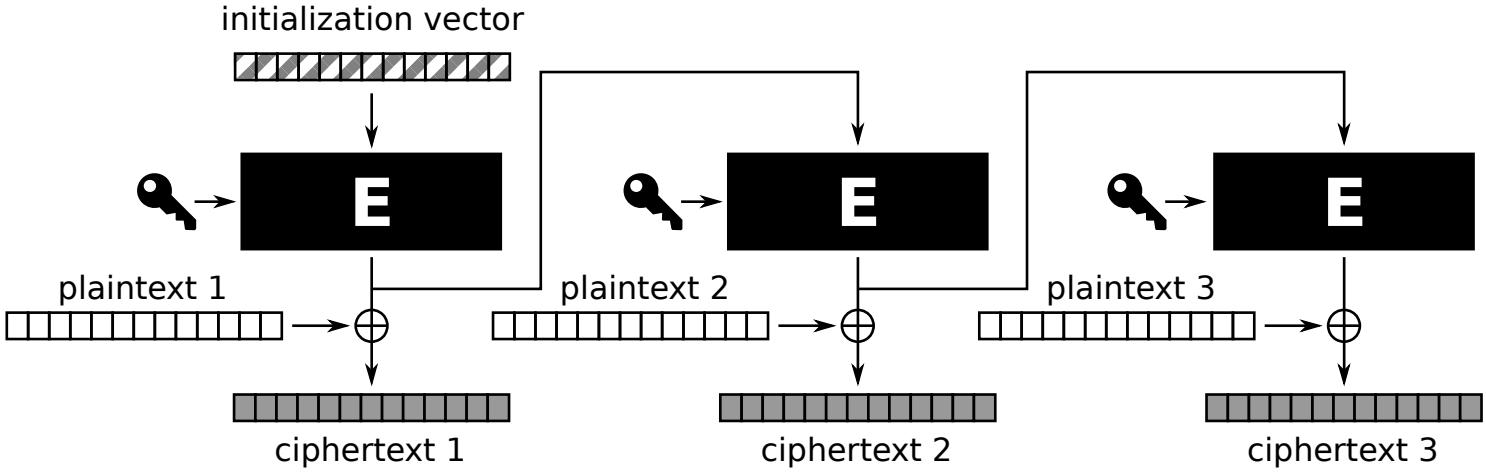
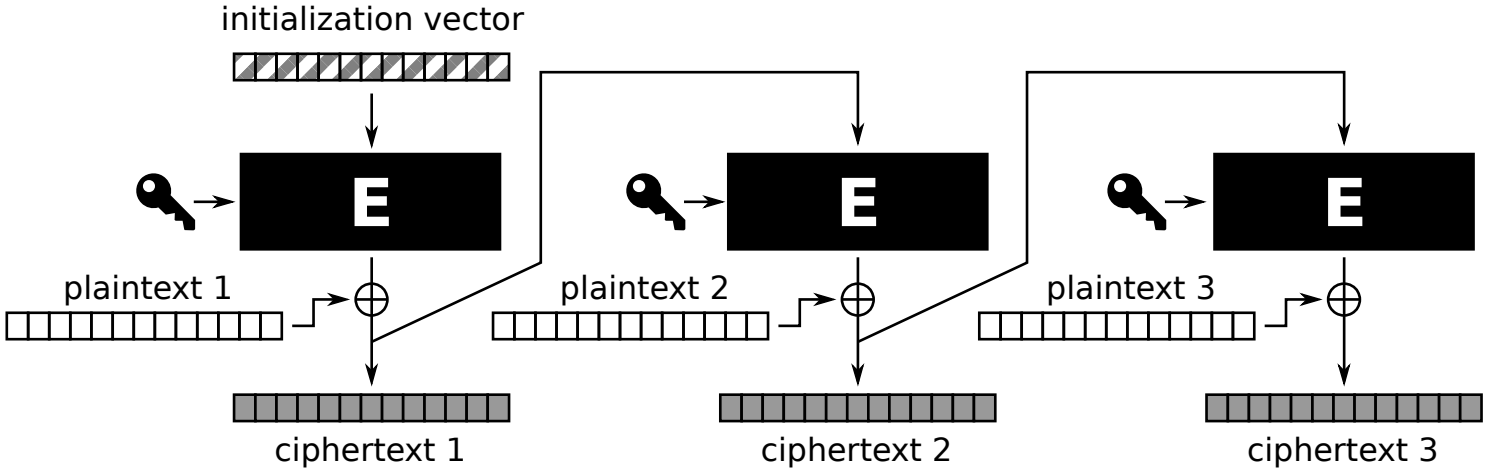
Cipher Block Chaining mode (**CBC**)



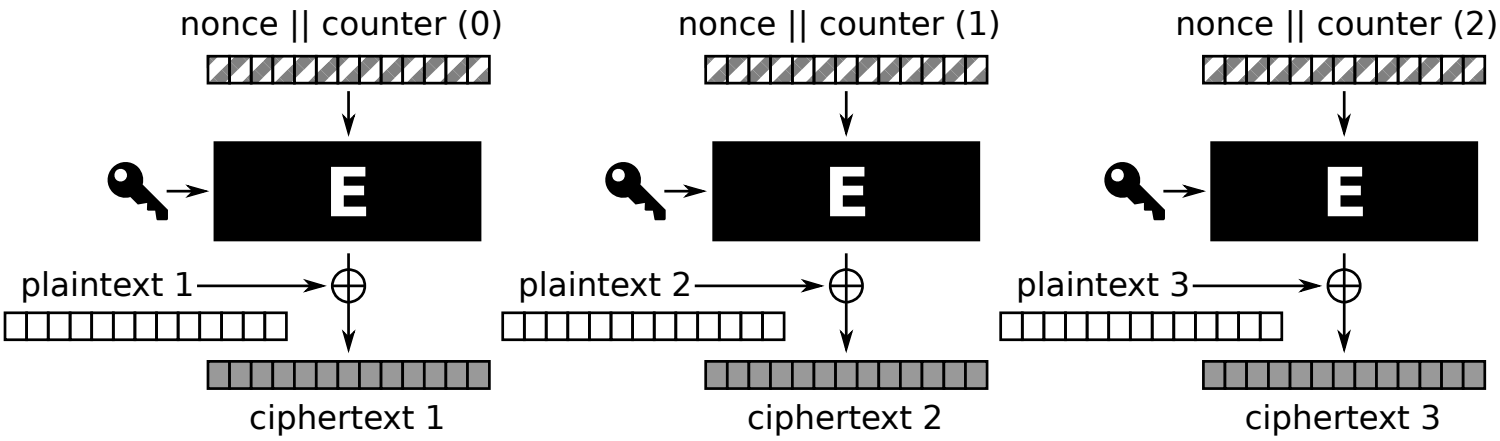
Output FeedBack mode (**OFB**)



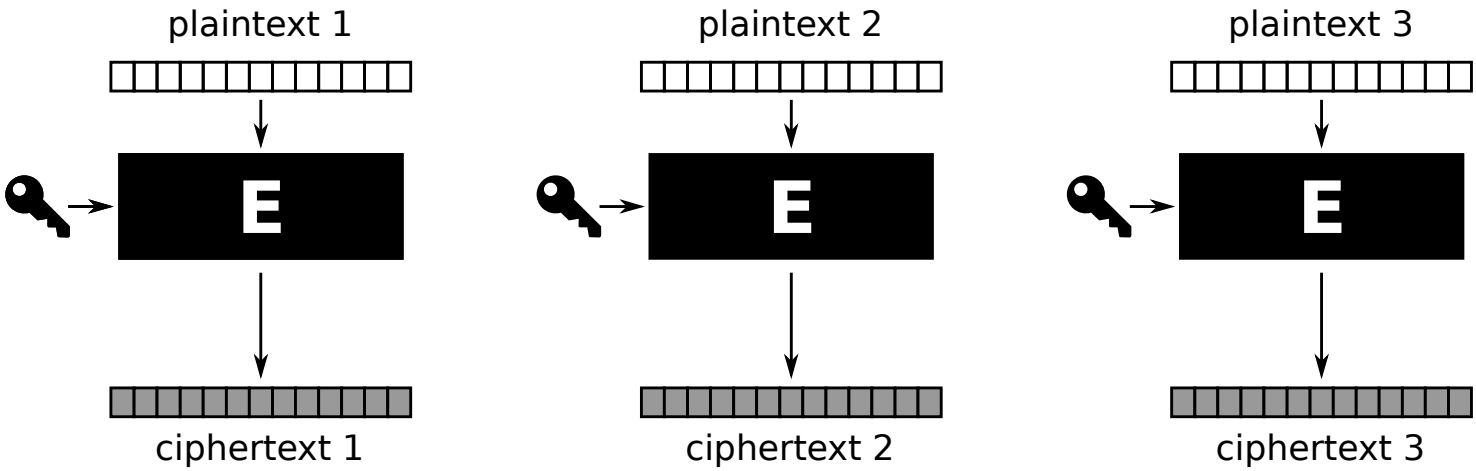
Cipher FeedBack mode (**CFB**)



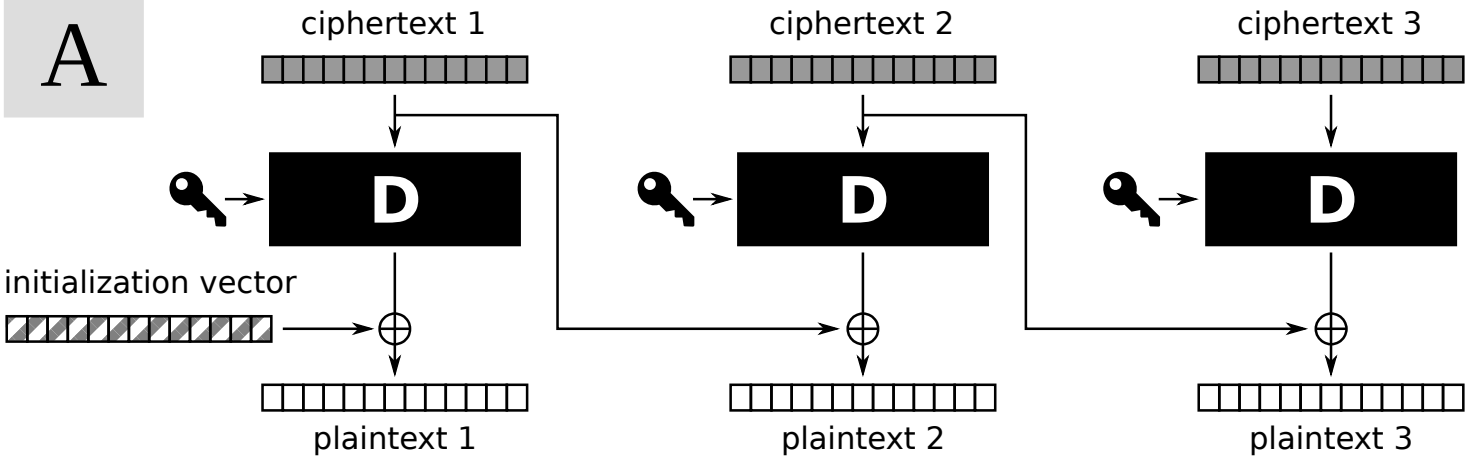
CounTeR mode (**CTR**)

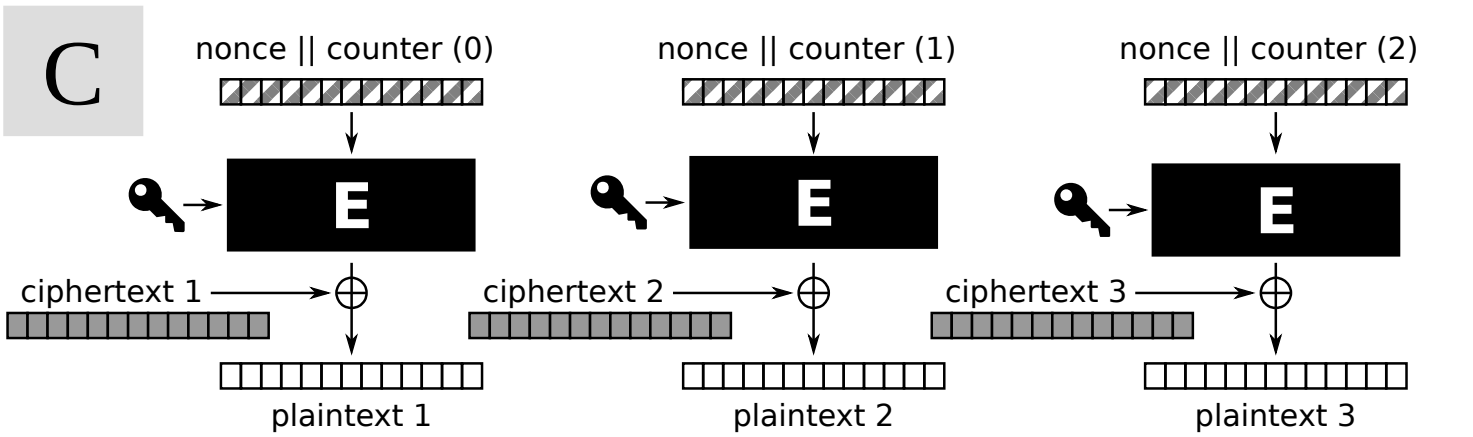


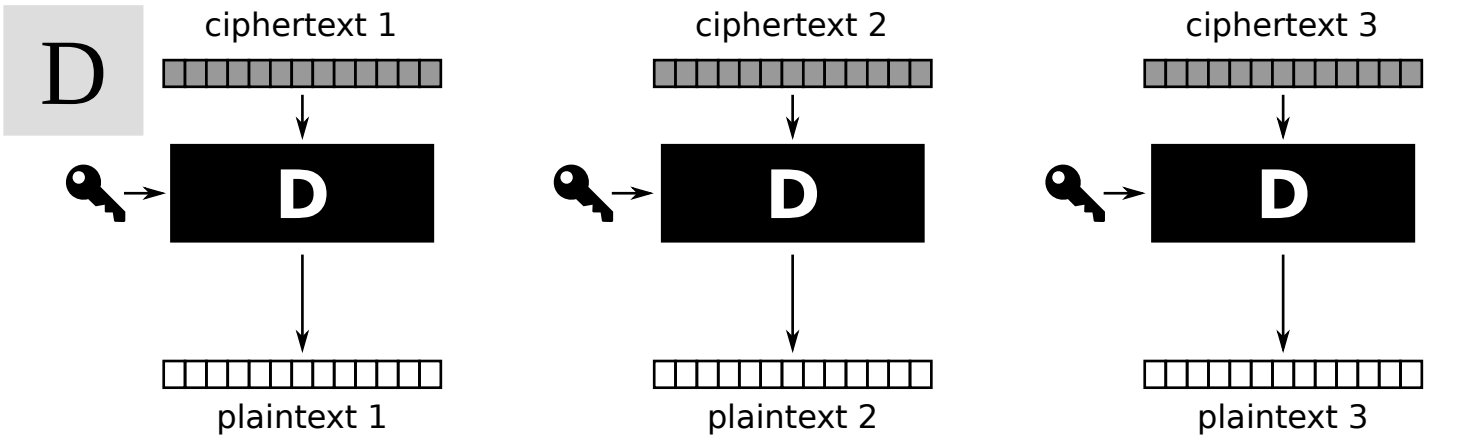
Electronic Code Book mode (**ECB**)

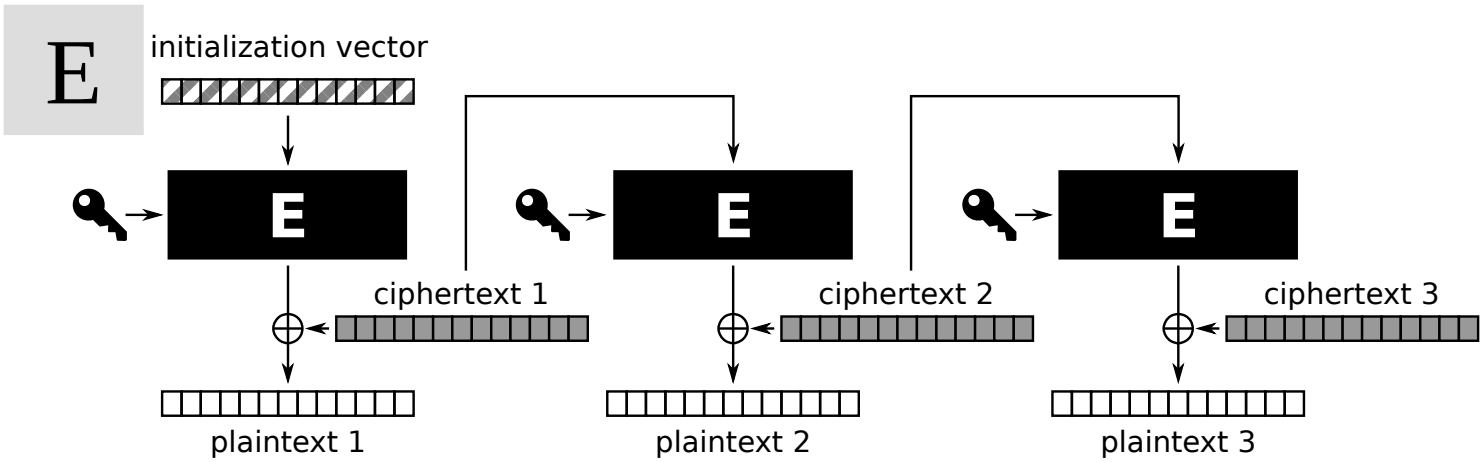


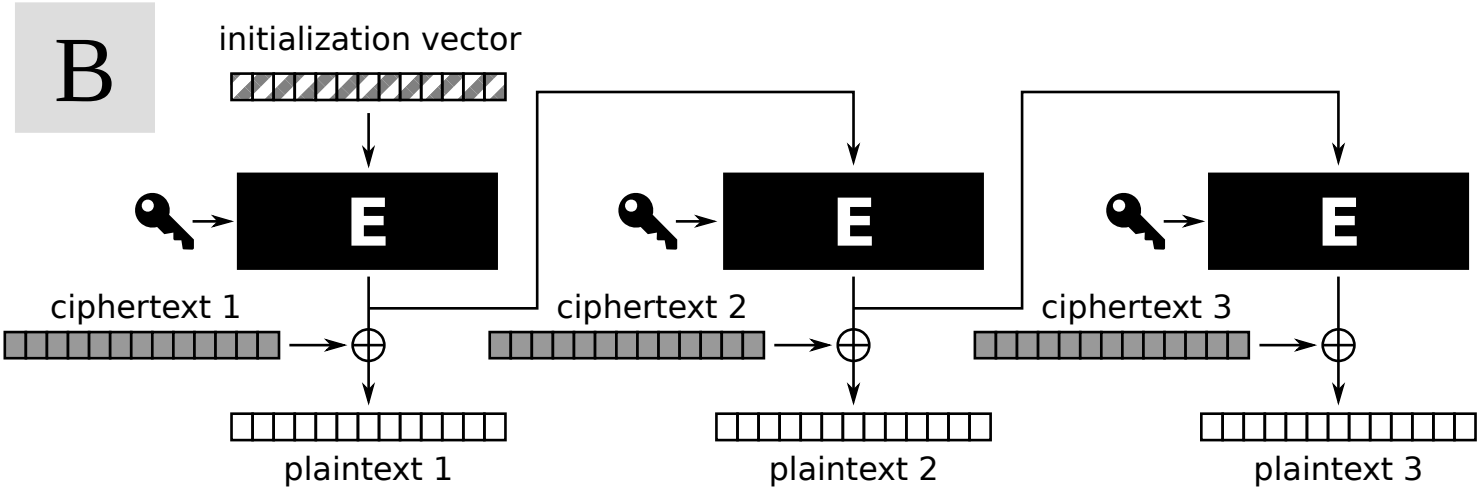
A




C
nonce || counter (0)
nonce || counter (1)
nonce || counter (2)
E
E
E
ciphertext 1
ciphertext 2
ciphertext 3
plaintext 1
plaintext 2
plaintext 3


D
ciphertext 1
ciphertext 2
ciphertext 3
D
D
D
plaintext 1
plaintext 2
plaintext 3


E
initialization vector
E
E
E
ciphertext 1
ciphertext 2
ciphertext 3
plaintext 1
plaintext 2
plaintext 3


B
initialization vector
E
E
E
ciphertext 1
ciphertext 2
ciphertext 3
plaintext 1
plaintext 2
plaintext 3

Use case:

You are submiting electronic voting ballot (exactly 3 bytes).

Use case:

You want to add privacy to instant messaging application.

Use case:

The customer wants the configuration of the program you develop to be saved in an encrypted form.

Use case:

You need to encrypt huge file backups.

Use case:

You need to encrypt the outgoing stream of video.

Use case:

You are adding encryption capabilities to new chips embedded into parking gate remote controls.

Feature 1:

The encryption process can be parallelised easily.

Feature 1:

The encryption process can be parallelised easily.

Feature 2:

The change in 1 ciphertext block causes 1 corrupted plaintext block.

Feature 2:

The change in 1 ciphertext block causes 1 corrupted plaintext block.

Feature 2:

The change in 1 ciphertext block causes 1 corrupted plaintext block.

Feature 3:

The change in 1 ciphertext block causes 2 corrupted plaintext blocks.

Feature 3:

The change in 1 ciphertext block causes 2 corrupted plaintext blocks.

Feature 4:

Encrypting the same plaintexts produces the same ciphertexts.

Feature 5:

Encryption/decryption can be accelerated by precomputation.

Feature 5:

Encryption/decryption can be accelerated by precomputation.

---------- extra ½ page (and ½ next page) ----------

Feature 4:

Encrypting the same plaintexts produces the same ciphertexts.

Feature 5:

Encryption/decryption can be accelerated by precomputation.

Feature 5:

Encryption/decryption can be accelerated by precomputation.

Feature 6 (bonus):

The plaintext block is corrupted predictably.

(predictability = changing some bits in ciphertext causes changes in the same positions in plaintext)

Feature 6 (bonus):

The plaintext block is corrupted predictably.

(predictability = changing some bits in ciphertext causes changes in the same positions in plaintext)

Feature 6 (bonus):

The plaintext block is corrupted predictably.

(predictability = changing some bits in ciphertext causes changes in the same positions in plaintext)

Feature 6 (bonus):

The plaintext block is corrupted predictably.

(predictability = changing some bits in ciphertext causes changes in the same positions in plaintext)

Feature 6 (bonus):

The plaintext block is corrupted predictably.

(predictability = changing some bits in ciphertext causes changes in the same positions in plaintext)

Feature 6 (bonus):

The plaintext block is corrupted predictably.

(predictability = changing some bits in ciphertext causes changes in the same positions in plaintext)

Feature 6 (bonus):

The plaintext block is corrupted predictably.

(predictability = changing some bits in ciphertext causes changes in the same positions in plaintext)

Feature 7 (bonus):

The plaintext block is corrupted UNpredictably.

(unpredictability = changing some bits in ciphertext causes random changes in plaintext)

Feature 7 (bonus):

The plaintext block is corrupted UNpredictably.

(unpredictability = changing some bits in ciphertext causes random changes in plaintext)

Feature 7 (bonus):

The plaintext block is corrupted UNpredictably.

(unpredictability = changing some bits in ciphertext causes random changes in plaintext)

Feature 8 (bonus):

Block synchronization is required.

(e.g. getting ciphertext blocks 1, 2, 4, 5, 6, … and thinking it's 1, 2, 3, 4, 5, … causes ALL remaining plaintext to be unreadable)

Feature 8 (bonus):

Block synchronization is required.

(e.g. getting ciphertext blocks 1, 2, 4, 5, 6, … and thinking it's 1, 2, 3, 4, 5, … causes ALL remaining plaintext to be unreadable)