Block cipher and modes of encryptions

Block cipher

- Other name for fixed-length encryption scheme

Problem with just encrypting each block of the message using a randomized encryption scheme

- Each block uses k bits of randomness
  - If we have d blocks, it requires dk bits of randomness.

- Randomness is expensive

Solution to minimize randomness

- Create an initial state
  - May use some randomness (called Nonce or IV).
- Encrypt the current block using the current state
- Update the state after each use of the block cipher

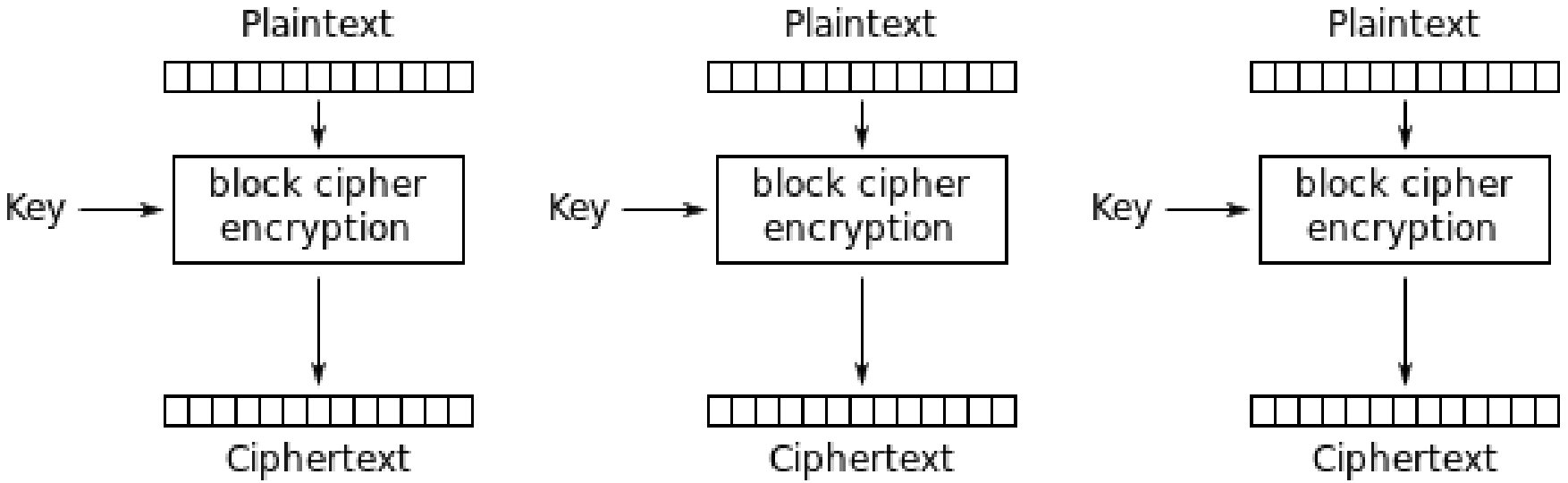
Goals (block cipher)

- Security
  - Is it secure?
  - What level of security does it have?
- Parallelizable: Can we encrypt/decrypt each block in parallel
  - We don’t need to wait for the previous part to encrypt the next part.
- Forward: Do we need to use decryption operation
  - Better if we don’t
- Error-resilient: If one block of the ciphertext becomes corrupted

ECB mode

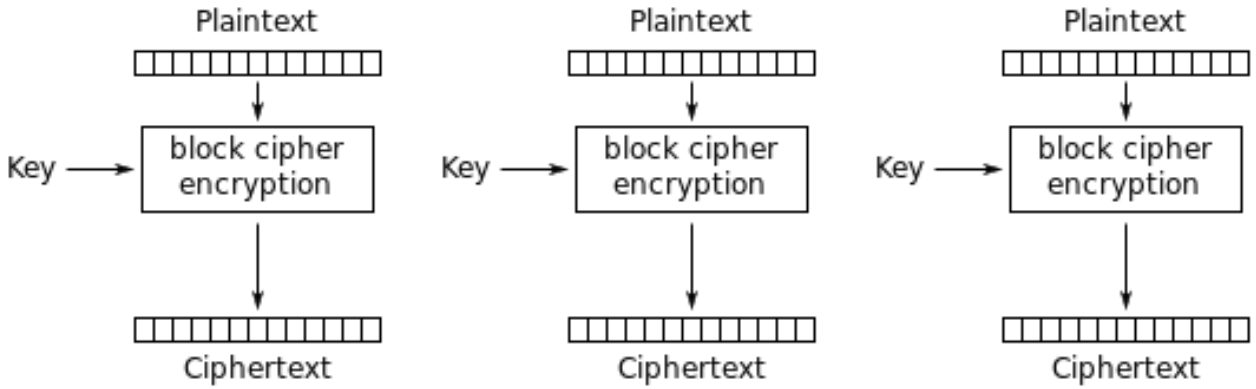
- $Init()$
  - $S_1 \leftarrow 0$
- $Output(m_i, S_i)$
  - $c_i \leftarrow Enc_k(m_i)$
- $Update(m_i, s_i)$
  - $S_{i+1} \leftarrow S_i$

Electronic codebook mode (ECB)



Electronic Codebook (ECB) mode encryption

Electronic codebook mode (ECB)

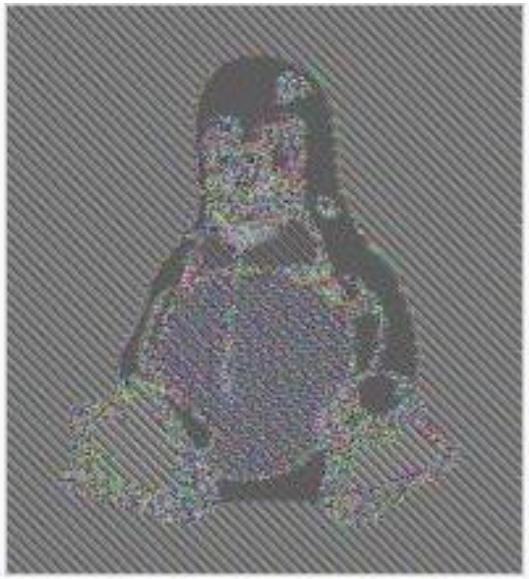


Electronic Codebook (ECB) mode encryption

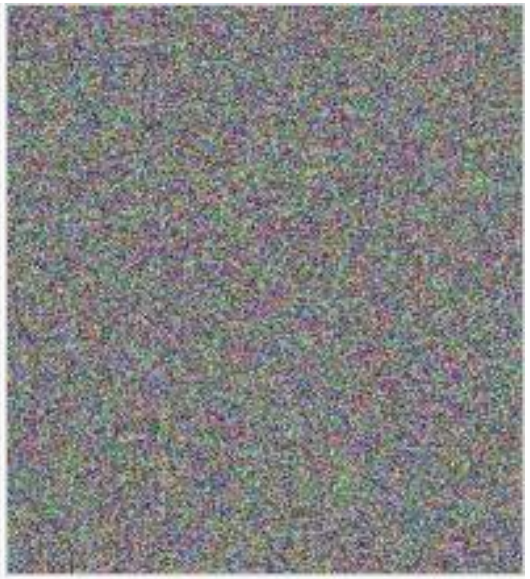
Secure?	Parallelizable	Forward	Error-resilient
No	yes	no	yes
Unless the plaintext has high entropy.			

Problem with ECB mode

Original image



Encrypted using ECB mode

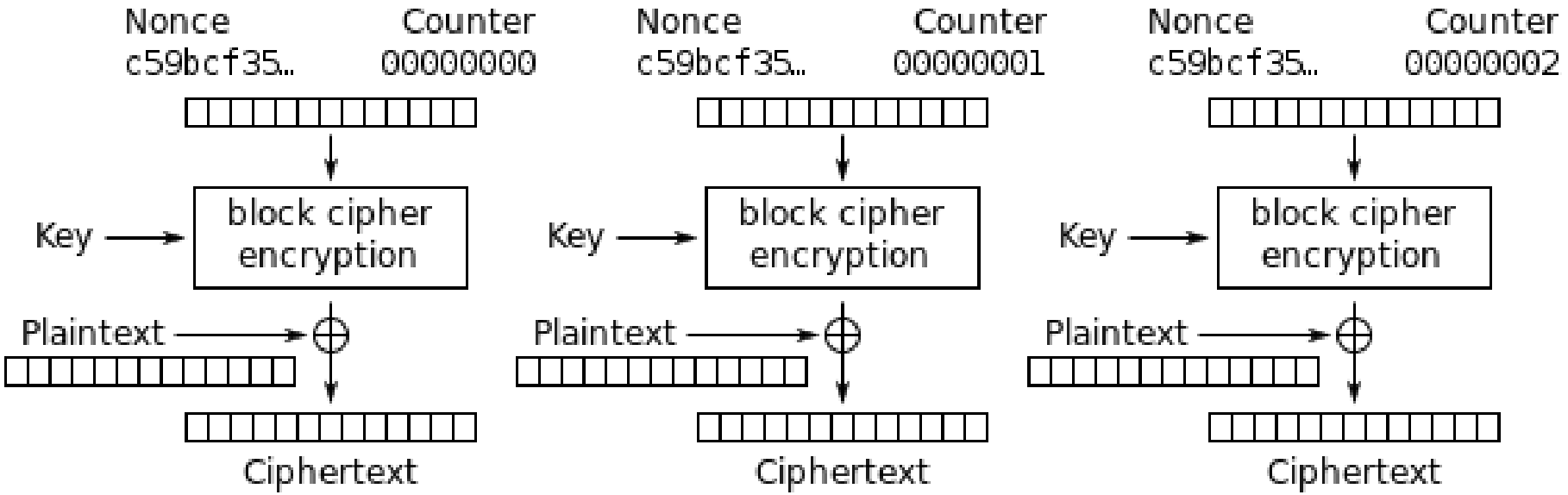


Modes other than ECB result in pseudo-randomness

Counter mode (CM)

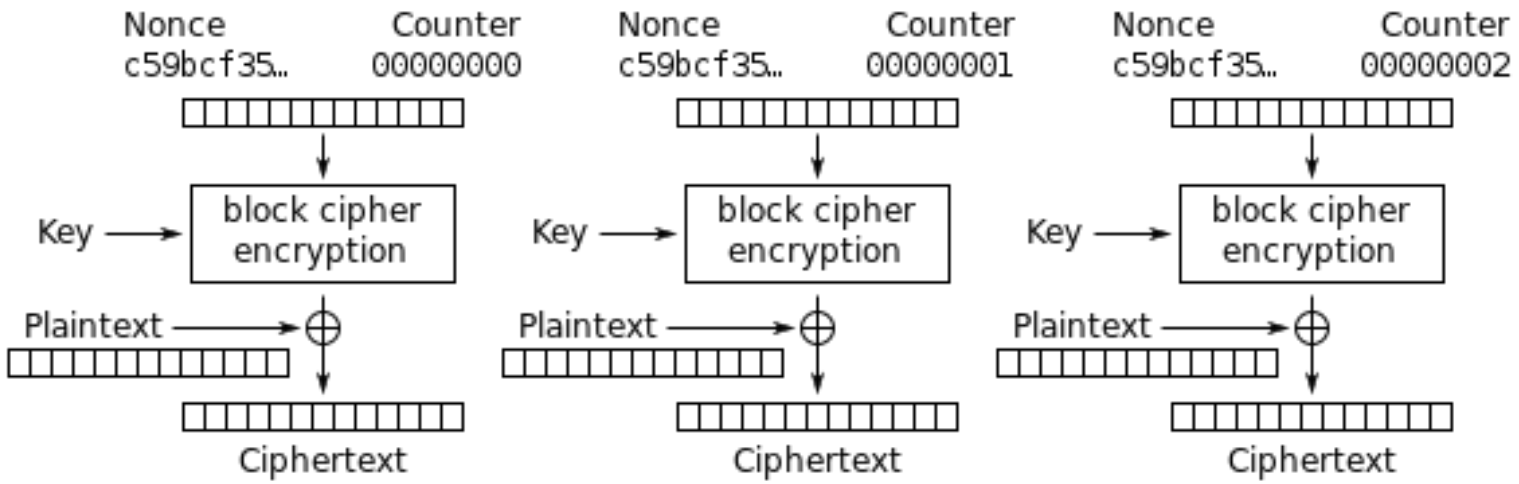
- $Init()$
  - $nonce \in_R \{0,1\}^{s/2}$
  - $S_1 \leftarrow (nonce, \{0\}^{s/2})$
- $Output(m_i, S_i)$
  - $c_i \leftarrow Enc_k(S_i) \oplus m_i$
- $Update(m_i, s_i)$
  - $s_{i+1} \leftarrow s_i + 1$

Counter mode (CM)



Counter (CTR) mode encryption

Counter mode



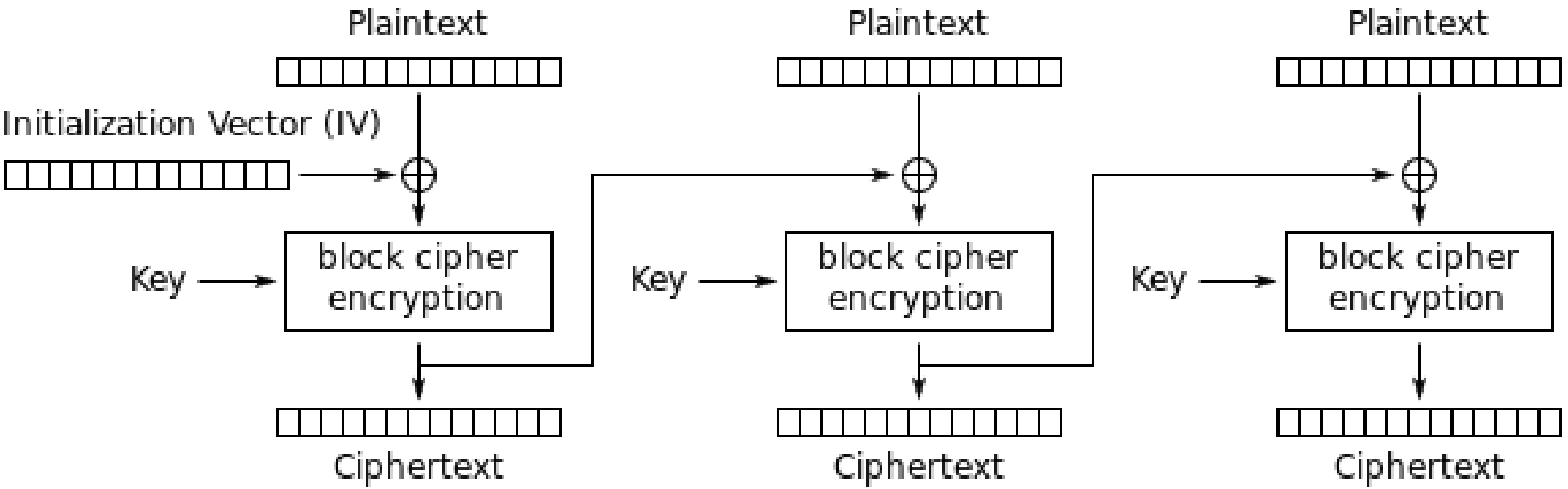
Counter (CTR) mode encryption

Secure?	Parallelizable	Forward	Error-resilient
Yes but	yes	yes	yes
IV security reduced by half			

Cipher block chaining

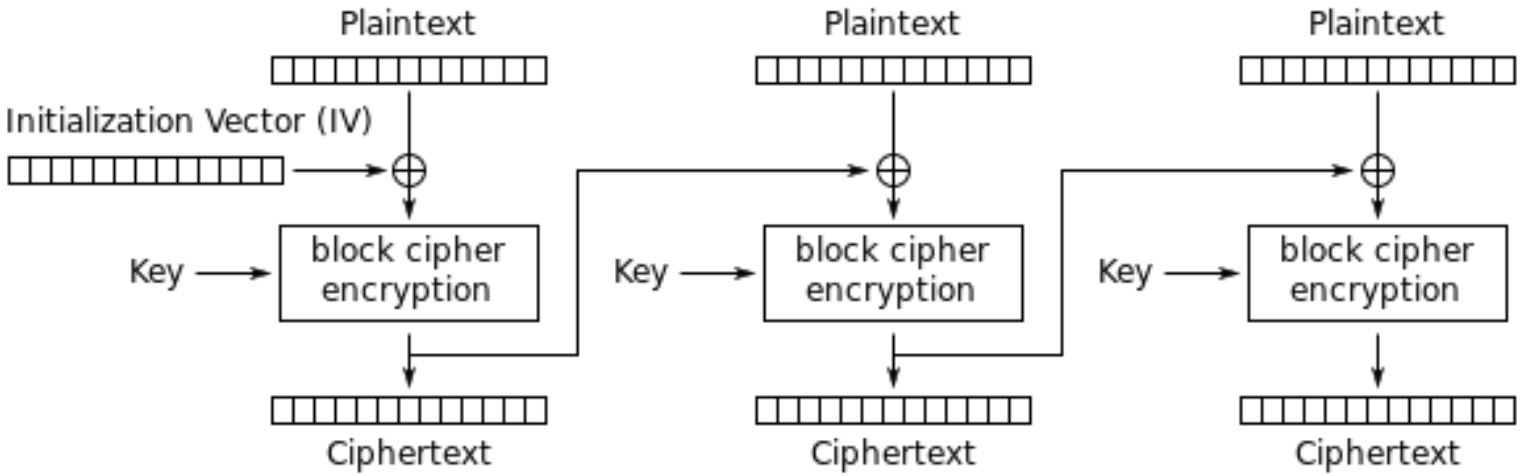
- $Init()$
  - $IV \in_R \{0,1\}^s$
  - $S_1 \leftarrow IV$
- $Output(m_i, S_i)$
  - $c_i \leftarrow Enc_k(m_i \oplus S_i)$
- $Update(m_i, s_i)$
  - $s_{i+1} \leftarrow c_i$

Cipher block chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

Cipher block chaining



Cipher Block Chaining (CBC) mode encryption

Secure?	Parallelizable	Forward	Error-resilient
Yes	no	no	no