Modes of operation

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Background

- Block ciphers encrypt block of b bits:

$$\mathrm{Enc} : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n, \quad \mathrm{Enc}_k(m) = c.$$

- Split longer messages into blocks of b bits; append padding: $\mathrm{pad}(m) = M_0\, M_1\, M_2 \ldots M_{t-1}$; M_{t-1} may include padding.
- Simplest mode is electronic codebook mode (ECB): encrypt blocks independently.

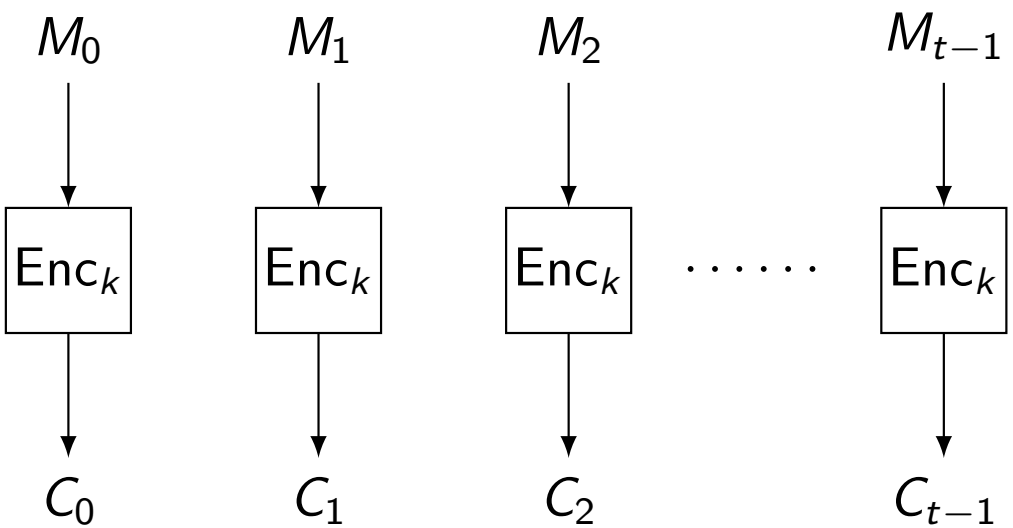


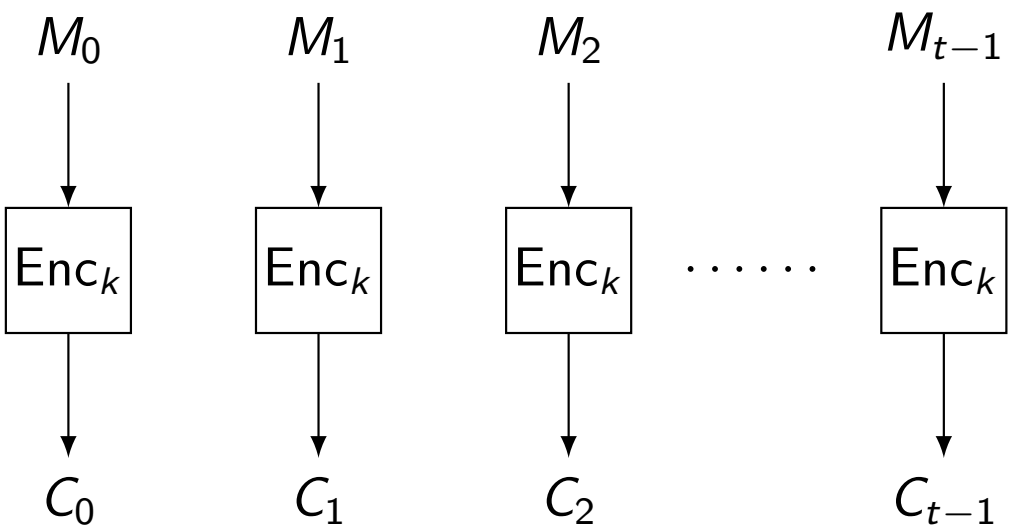
Image credits: ECB mode: adapted from Jérémy Jean, ECB penguin: By en:User:Lunkwill

Background

- Block ciphers encrypt block of b bits:

$$\mathrm{Enc} : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n, \quad \mathrm{Enc}_k(m) = c.$$

- Split longer messages into blocks of b bits; append padding: $\mathrm{pad}(m) = M_0\, M_1\, M_2 \ldots M_{t-1}$; M_{t-1} may include padding.
- Simplest mode is electronic codebook mode (ECB): encrypt blocks independently.



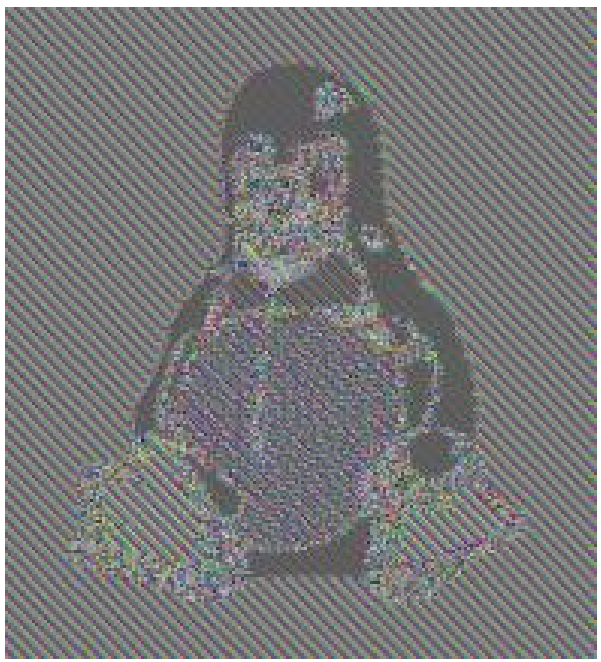


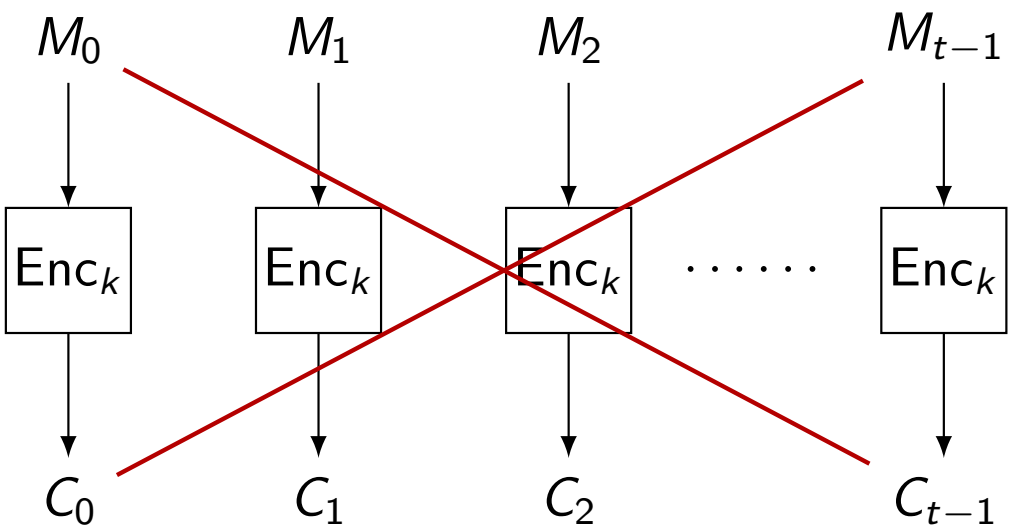
Image credits: ECB mode: adapted from Jérémy Jean, ECB penguin: By en:User:Lunkwill

Background

- Block ciphers encrypt block of b bits:

$$\mathrm{Enc} : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n, \quad \mathrm{Enc}_k(m) = c.$$

- Split longer messages into blocks of b bits; append padding: $\mathrm{pad}(m) = M_0\, M_1\, M_2 \ldots M_{t-1}$; M_{t-1} may include padding.
- Simplest mode is electronic codebook mode (ECB): encrypt blocks independently.



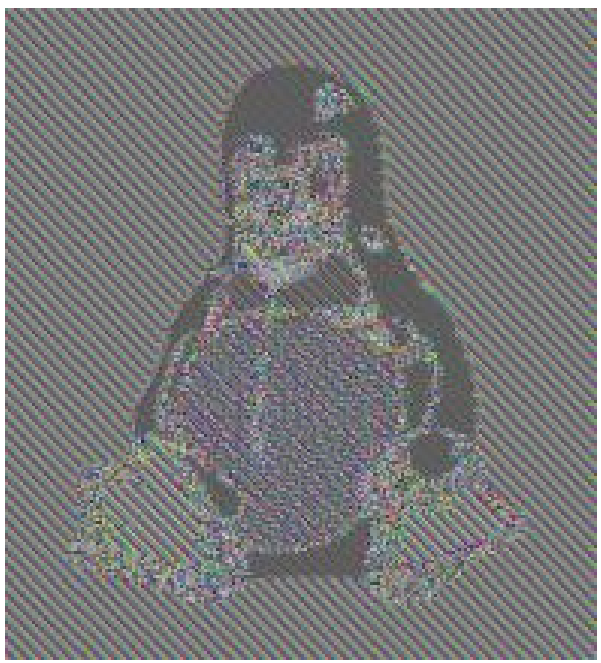
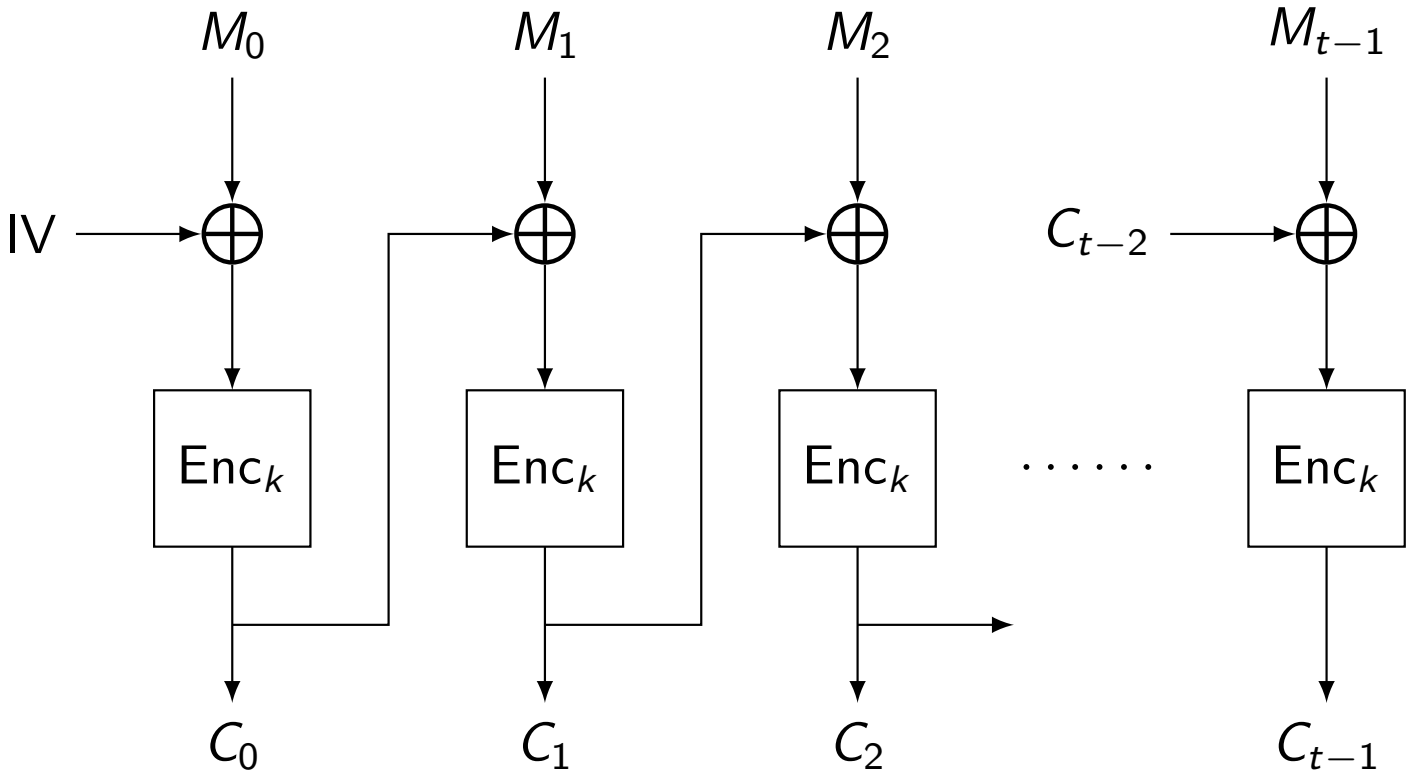


Image credits: ECB mode: adapted from Jérémy Jean, ECB penguin: By en:User:Lunkwill

Cipher-block-chaining mode (CBC)

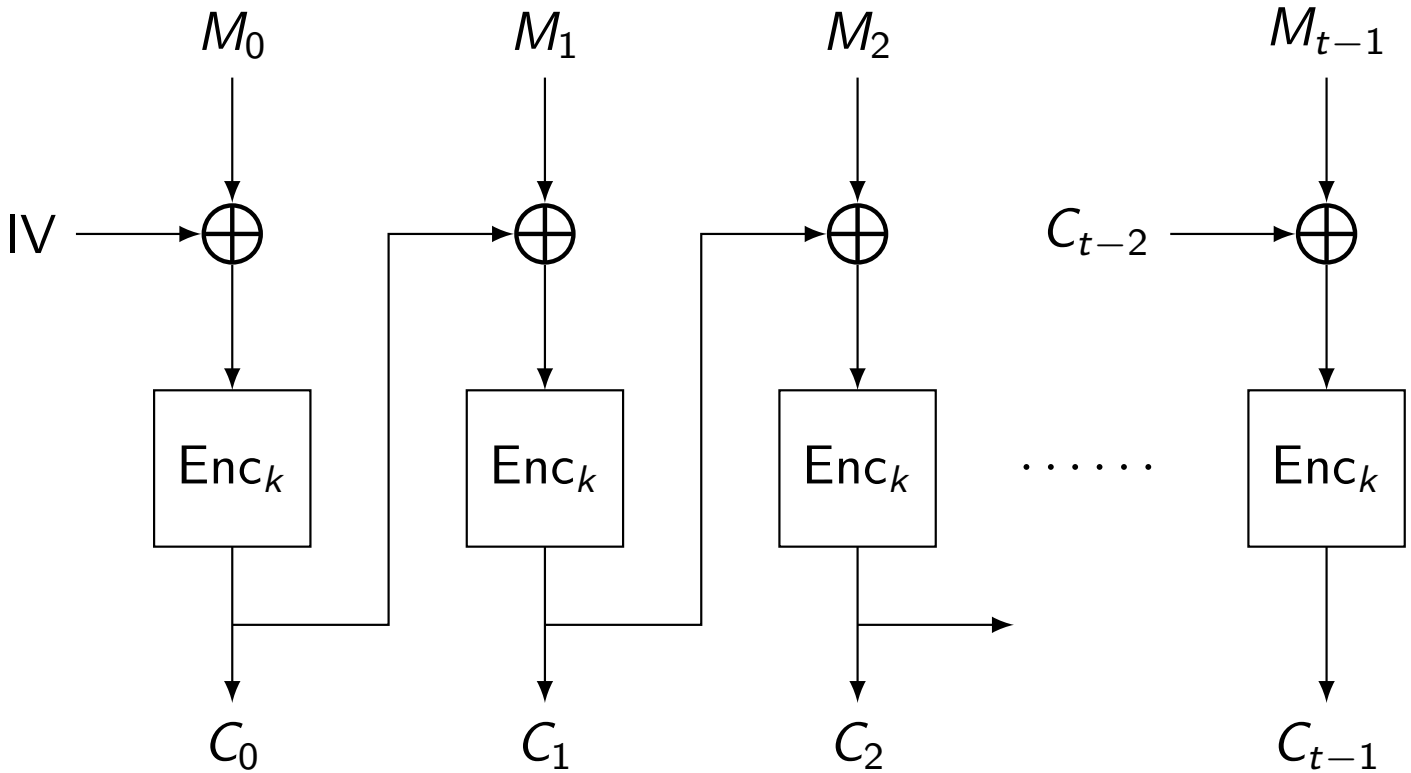


To encrypt message m under key k, pick IV and determine blocks M_i.

Then $C_0 = \mathrm{Enc}_k(M_0 + \mathrm{IV}), \quad C_i = \mathrm{Enc}_k(M_i + C_{i-1})$ for $i > 0$.

Send ciphertext IV $C_0\, C_1\, C_2 \ldots C_{t-1}$.

Cipher-block-chaining mode (CBC)



To encrypt message m under key k, pick IV and determine blocks M_i.

Then $C_0 = \mathrm{Enc}_k(M_0 + \mathrm{IV}), \quad C_i = \mathrm{Enc}_k(M_i + C_{i-1})$ for $i > 0$.

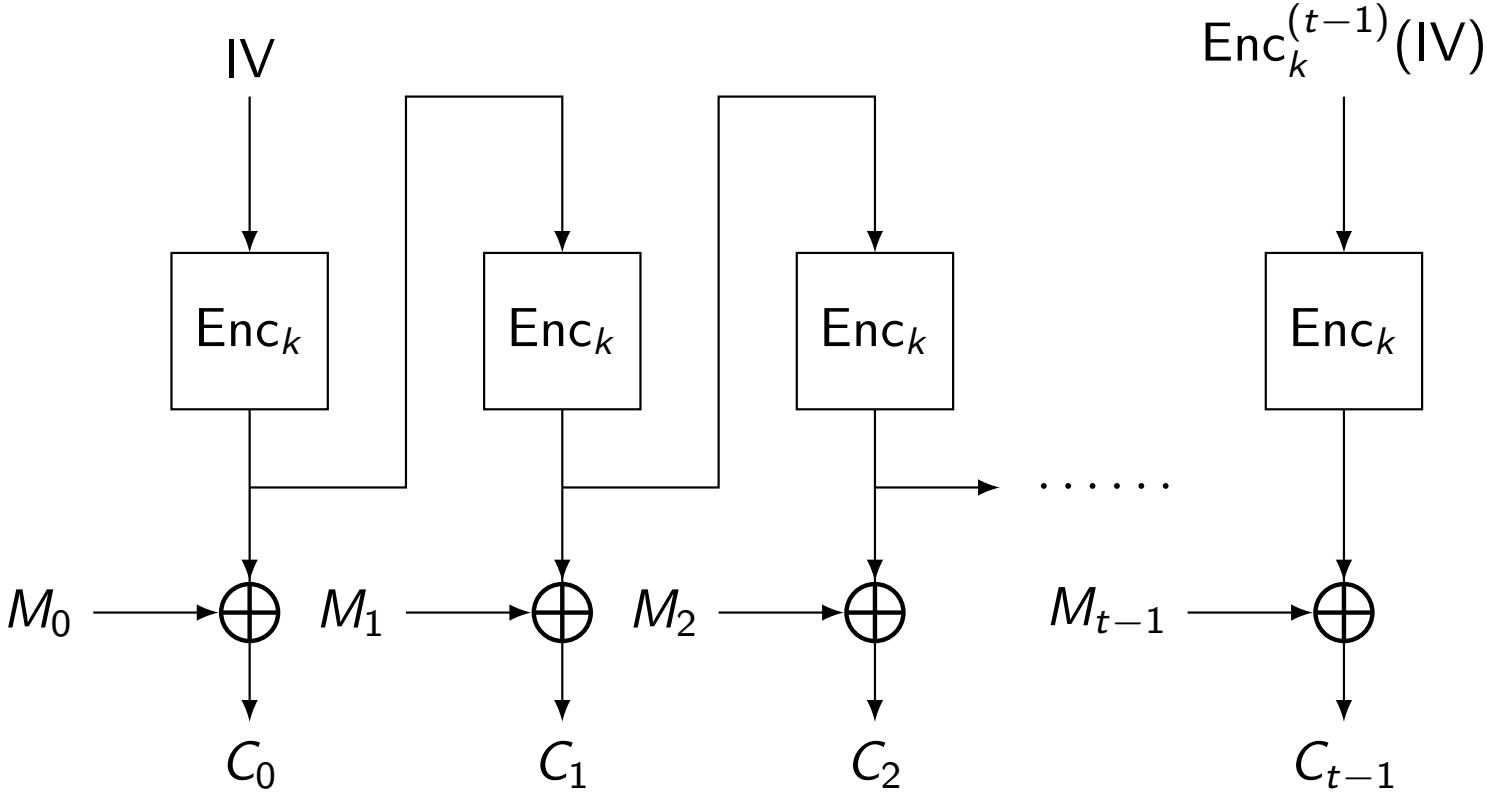
Send ciphertext IV $C_0\, C_1\, C_2 \ldots C_{t-1}$.

Decrypt: $M_0 = \mathrm{Dec}_k(C_0) + \mathrm{IV}, \quad M_i = \mathrm{Dec}_k(C_i) + C_{i-1}$ for $i > 0$.

To retrieve M_i we need only C_{i-1}, C_i: locally decryptable.

Image credit: adapted from Jérémy Jean

Output-feedback mode (OFB)



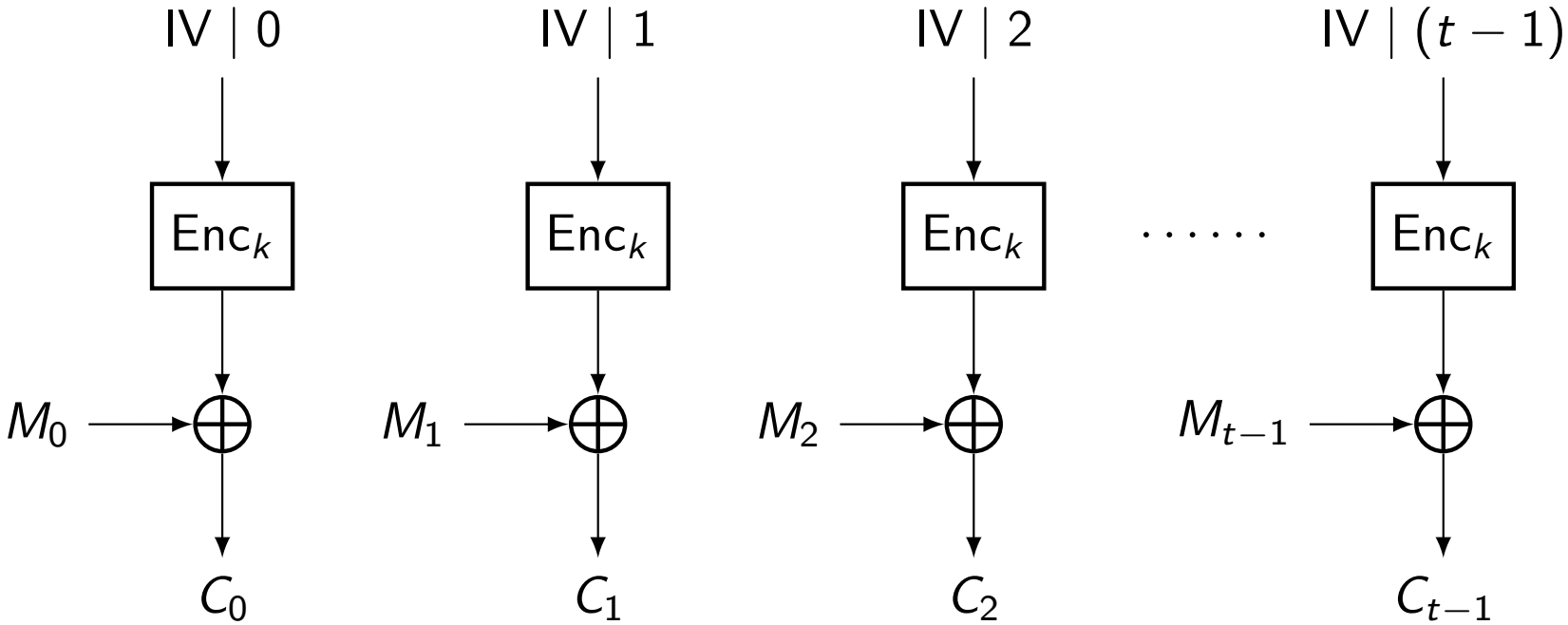
To encrypt, use: $C_i = M_i + \mathrm{Enc}_k^{i+1}(\mathrm{IV})$ for $i \geq 0$.

To decrypt, use:: $M_i = C_i + \mathrm{Enc}_k^{i+1}(\mathrm{IV})$ for $i \geq 0$.

- OFB does not require Dec_k.
- Encryption resembles data flow in stream cipher.
- Later blocks have higher cost, but $\mathrm{Enc}_k^{i+1}(\mathrm{IV})$ can be precomputed. (No dependence on M_i.)

Image credit: adapted from Jérémy Jean

Counter mode (CTR)



Here IV | i means writing i in binary and concatenating it with IV.
IV length limits space for counter. IV must not repeat.
Can use binary addition instead of concatenation.

To encrypt, use: $C_i = M_i + \mathrm{Enc}_k(\mathrm{IV} \mid i)$ for $i \geq 0$.

To decrypt, use:: $M_i = C_i + \mathrm{Enc}_k(\mathrm{IV} \mid i)$ for $i \geq 0$.

- CTR does not require Dec_k.
- Each block has same cost, can precompute encryption stream; can locally encrypt and decrypt.

Image credit: adapted from Jérémy Jean

Warnings!

- Always authenticate and check integrity!
  - Block ciphers need modes and MACs.
  - Stream ciphers need MACs.
- Typically, Alice and Bob share a key k from which encryption key k_{enc} and authentication key k_{auth} are computed.
  Example $k_{enc} = H(k\,0)$, $k_{auth} = H(k\,1)$.
- IV needs to be sent as part of the ciphertext.
  Most modes require non-repeating IVs (else two-time pad).
- There are more modes; many have issues with padding.
  (See homework 3 for an interesting case).

Warnings!

- Always authenticate and check integrity!
  - Block ciphers need modes and MACs.
  - Stream ciphers need MACs.
- Typically, Alice and Bob share a key k from which encryption key k_{enc} and authentication key k_{auth} are computed.
  Example $k_{enc} = H(k\,0)$, $k_{auth} = H(k\,1)$.
- IV needs to be sent as part of the ciphertext.
  Most modes require non-repeating IVs (else two-time pad).
- There are more modes; many have issues with padding.
  (See homework 3 for an interesting case).
- Modes like AES-GCM achieve authenticated encryption.
- Sometimes want to authenticate and protect integrity of more data than we encrypt, e.g., sequence numbers in protocols.
  Authenticated encryption with associated data (AEAD)
  is the right tool for this.
- AEAD can be built from pieces we know, but more efficient or more secure when purpose built, see the Caesar competition.