امنیت داده ها

فصل هفتم: زنجیره سازی بلوک های رمز

دکتر یعقوب فرجامی

عضو هیات علمی دانشکده فنی قم

- برخی مدهای کاری:
  - ECB: Electronic Code Book
  - CBC: Cipher Block Chaining
  - CTR: Counter Mode
  - CFB: Cipher Feed Back
  - OFB: Output Feed Back
- مدهای کاری را می توان با AES، DES، CAST-128 ... پیاده سازی کرد.

How to use DES boxes

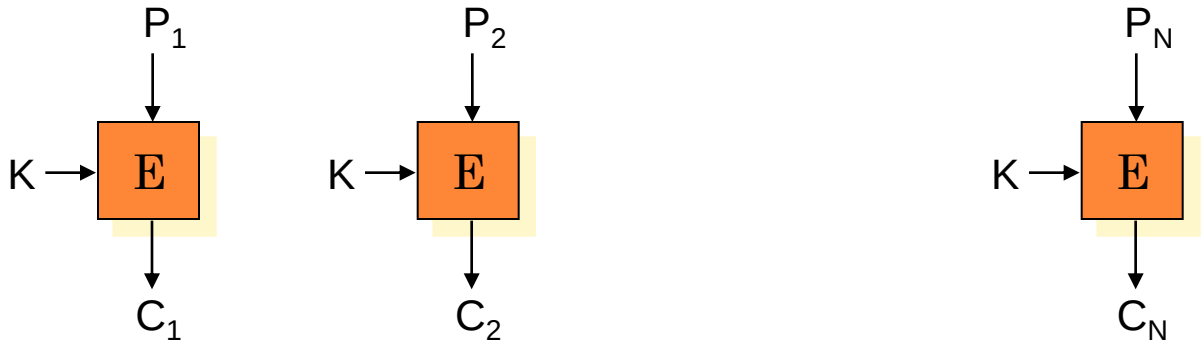
An lengthy message…. (>> 64 bits)

DES Encryption

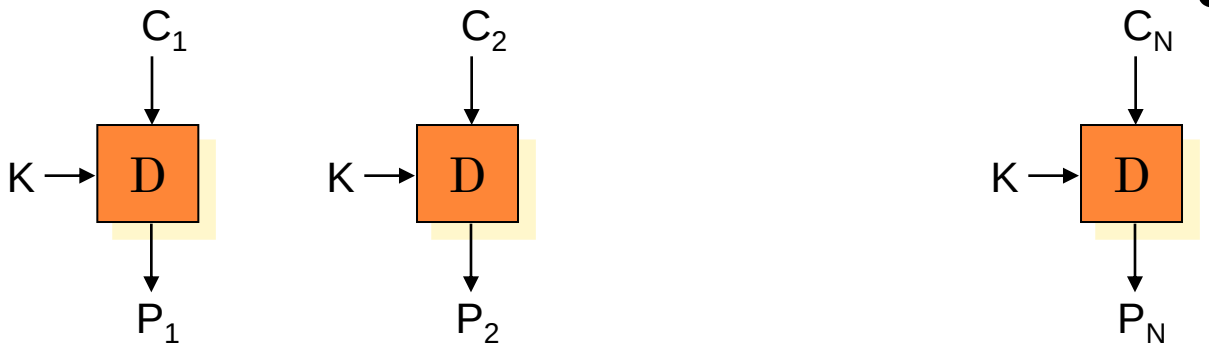
DES Decryption

مد کاری ECB

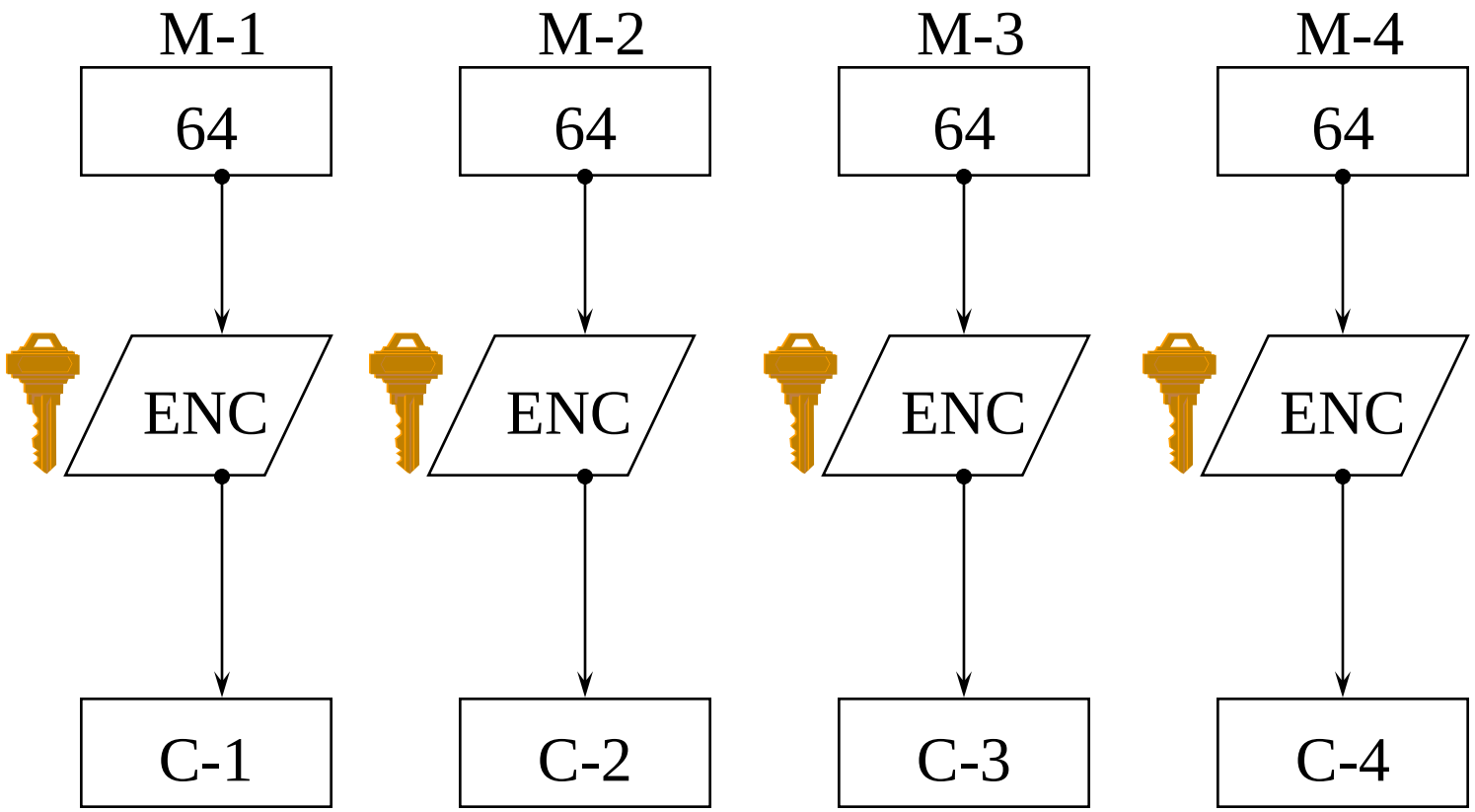
- رمز نگاری:



- رمز گشایی:

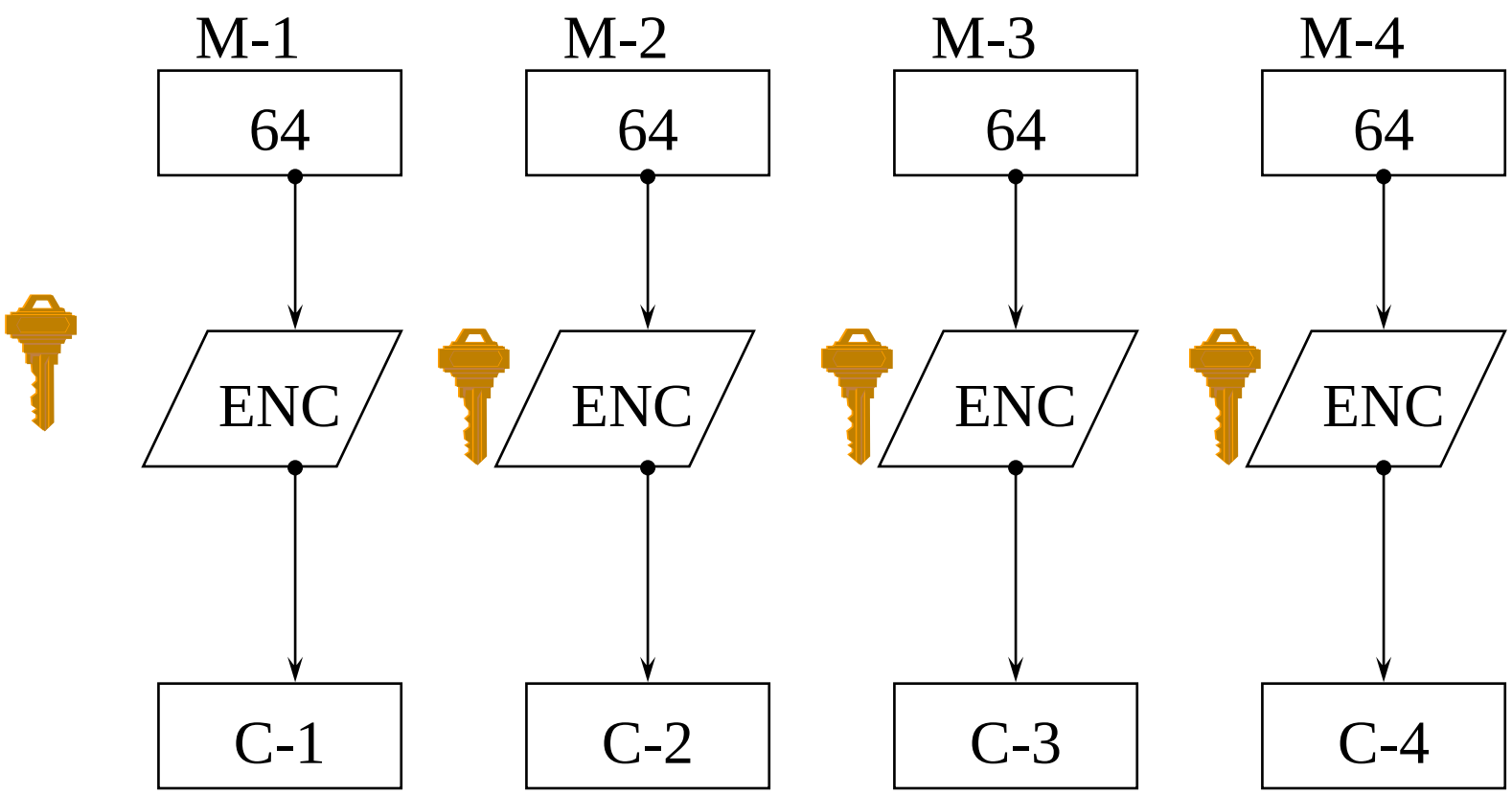


Electronic Code Book (ECB)



If we loss one C block, how many M blocks do we loss?

ECB's problem



If (M-1 == M-3), will (C-1 == C-3)?

بررسی مد کاری ECB

- اشکال اساسی: هر متن واضح به ازاء کلید ثابت همیشه به یک متن رمز شده نگاشته میشود.
  - دشمن میتواند دریابد که پیامهای یکسان ارسال شده اند.

این مد امن محسوب نمیشود حتی اگر از یک رمز قطعه ایی قوی استفاده کنیم.

- ECB مثالی از مواردی است که علی رغم بهره برداری از عناصر مرغوب، کیفیت نهایی دلخواه نیست.

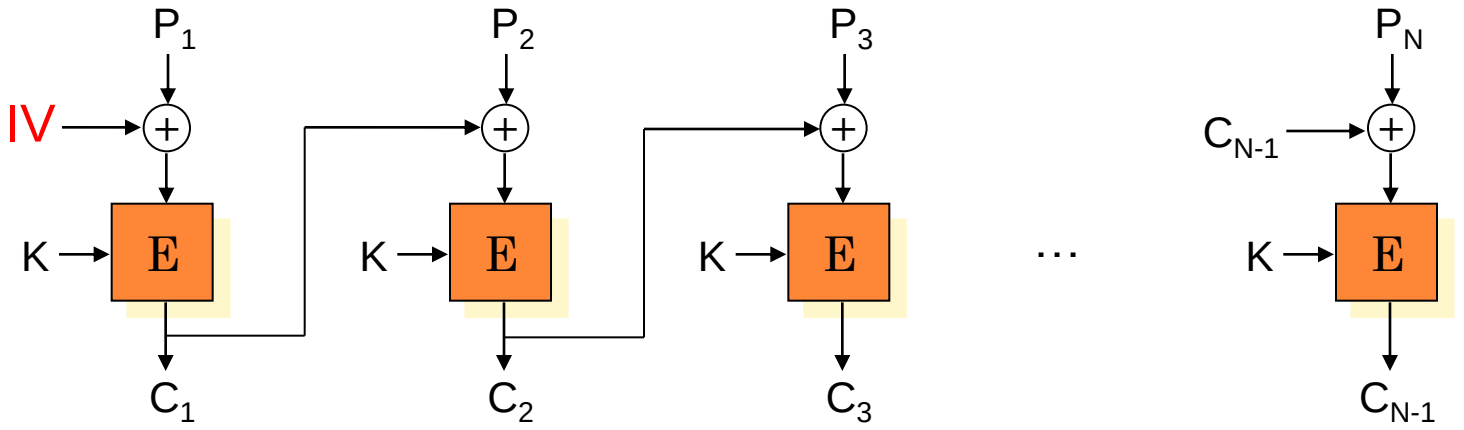
ECB's problem

- مشکل در ارسال یک تصویر رمز شده
  - چون تمام پیکسل ها با یک شیفت مشابه به حالت دیگری رسیده اند، کل تصویر قابل شناسایی است
- دسترسی نفوذ گر به دیتابیس
  - حتی اگر نفوذ گر از داده ها هم چیزی دستگیرش نشود به علت مشخص بودن تک تک فیلدها امکان جابه جایی آن ها وجود خواهد داشت (حمله از نوع غیر فعال)

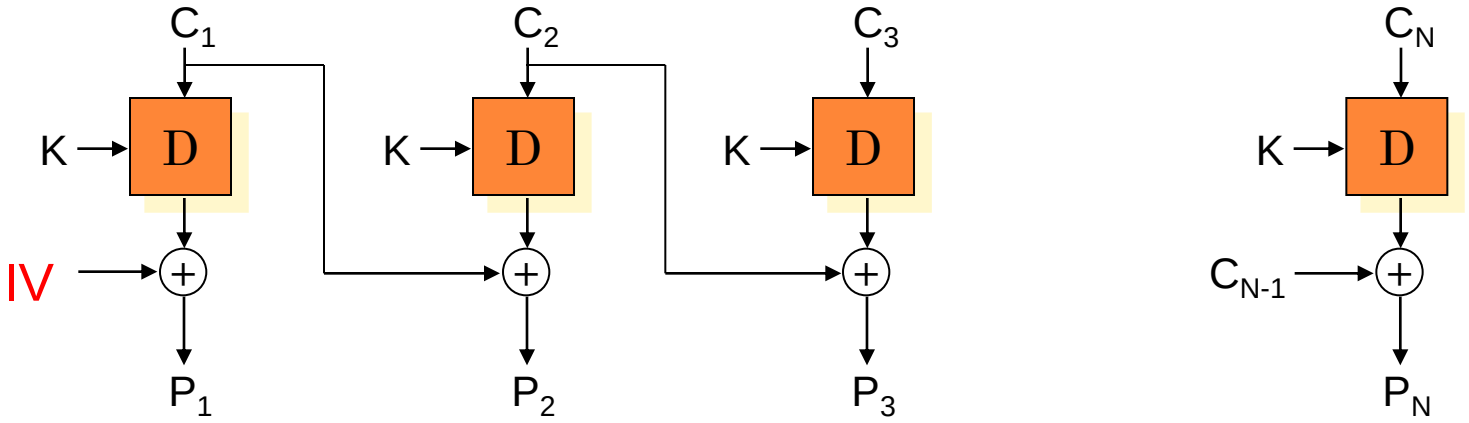
مد کاری CBC-1

- این مد از یک مقدار دهی اولیه تصادفی، IV، بهره میگیرد.
- مقدار IV در هر بار رمز نگاری به صورت تصادفی تغییر میکند.
- IV همراه با متن رمز شده به صورت واضح ارسال میشود.
- هر متن واضح به ازاء کلید ثابت هر بار به یک متن رمز شده متفاوت نگاشته میشود (زیرا مقدار IV تغییر مینماید).

- رمز نگاری:



- رمز گشایی:

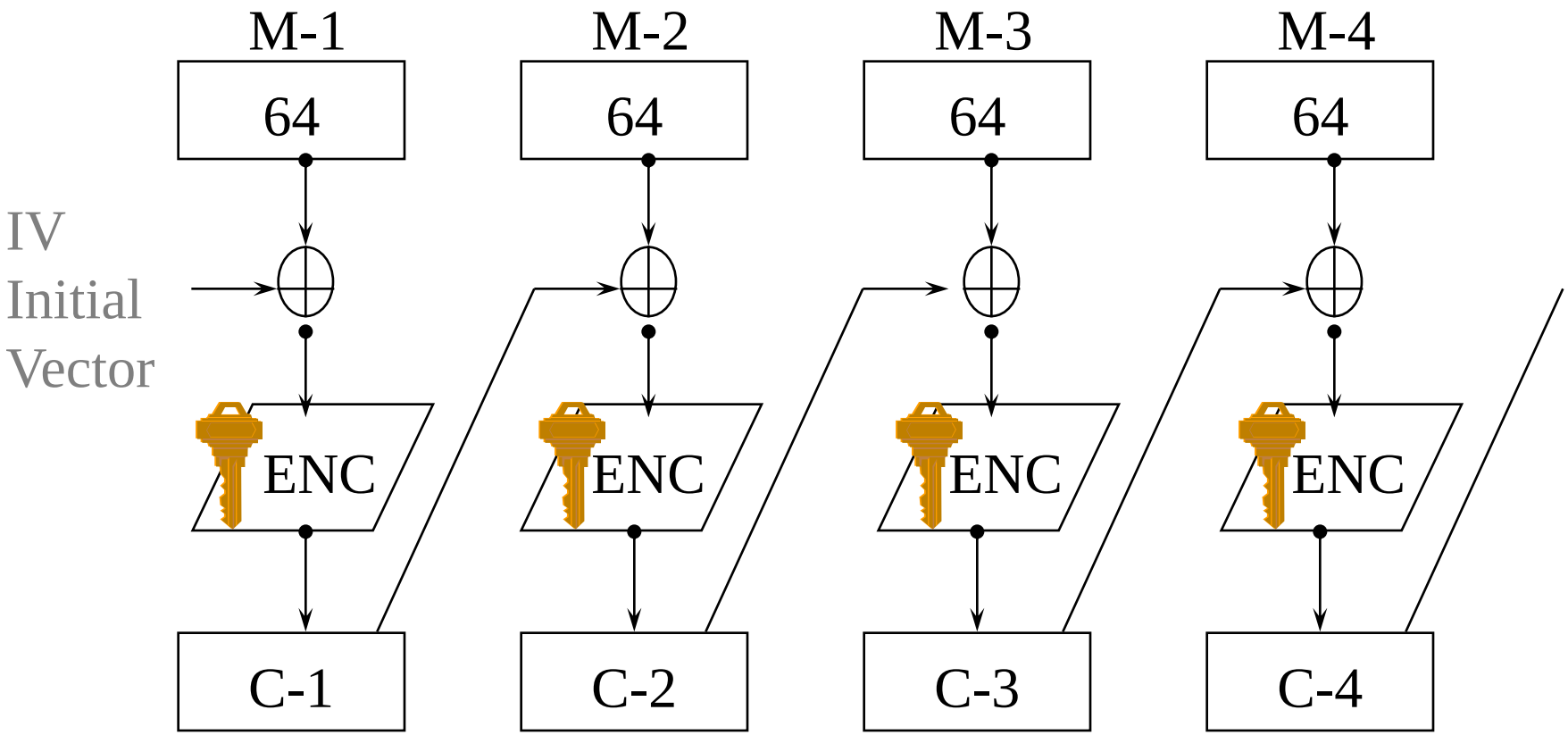


بررسی مد کاری CBC

- ملزومات امنیتی:
  - IV باید کاملاً غیر قابل پیش بینی باشد (برای تضمین عدم تشابه متن رمز پیام های یکسان)
- رمزنگاری:
  - عملیات رمزنگاری قابل موازی سازی نیست.
  - مقدار IV و متن واضح باید در دسترس باشند.

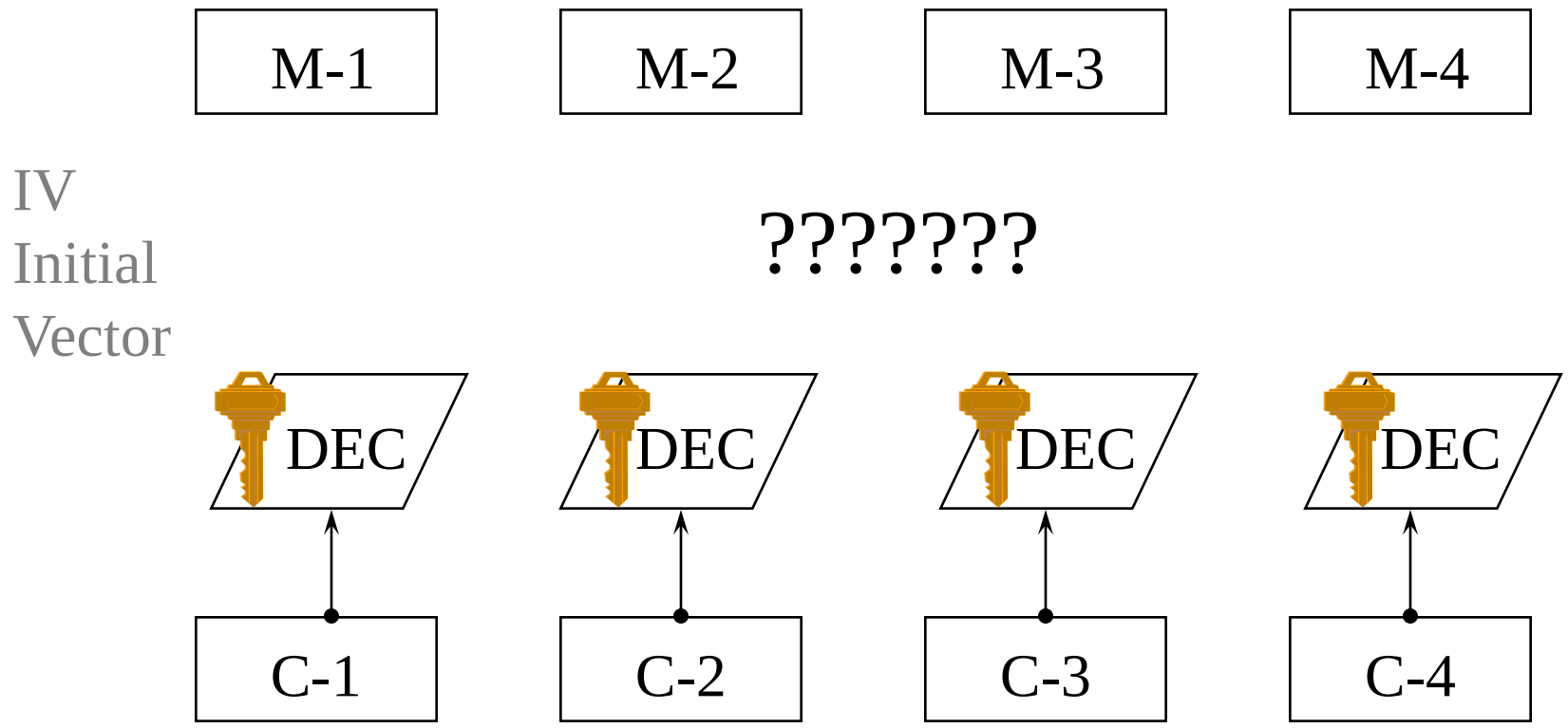
- رمزگشایی:
  - عملیات رمزگشایی قابل موازی سازی است.
  - مقدار IV و متن رمزشده باید در دسترس باشند.
- طول پیام:
  - در برخی موارد ممکن است وادار به افزایش طول پیام بشویم.
    - طول پیام باید مضربی از طول قطعه باشد.
- پیاده سازی:
  - رمز گشایی و رمز نگاری، هر دو باید پیاده سازی شوند.

Cipher Block Chaining (CBC)

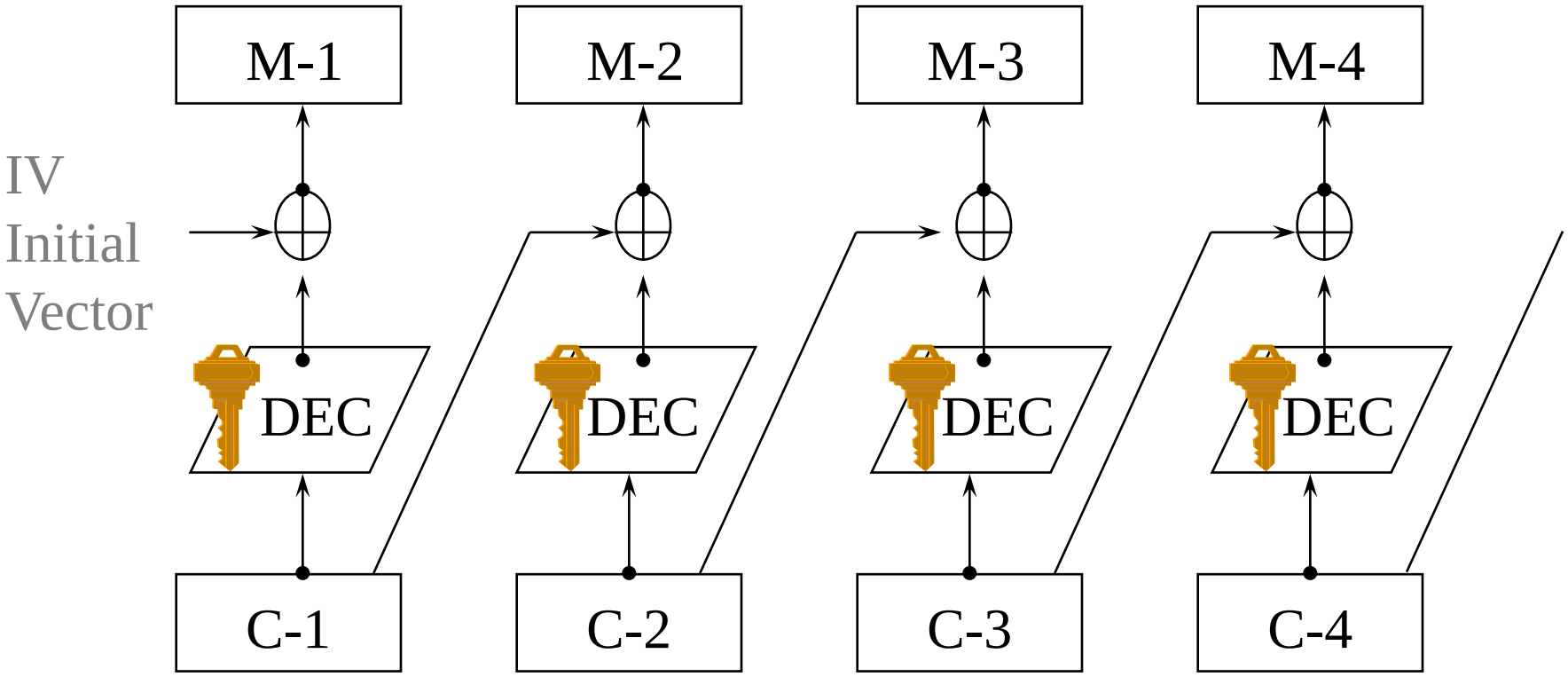


If (M-1 == M-3), will (C-1 == C-3) be likely?

How to decrypt CBC?



CBC Decryption



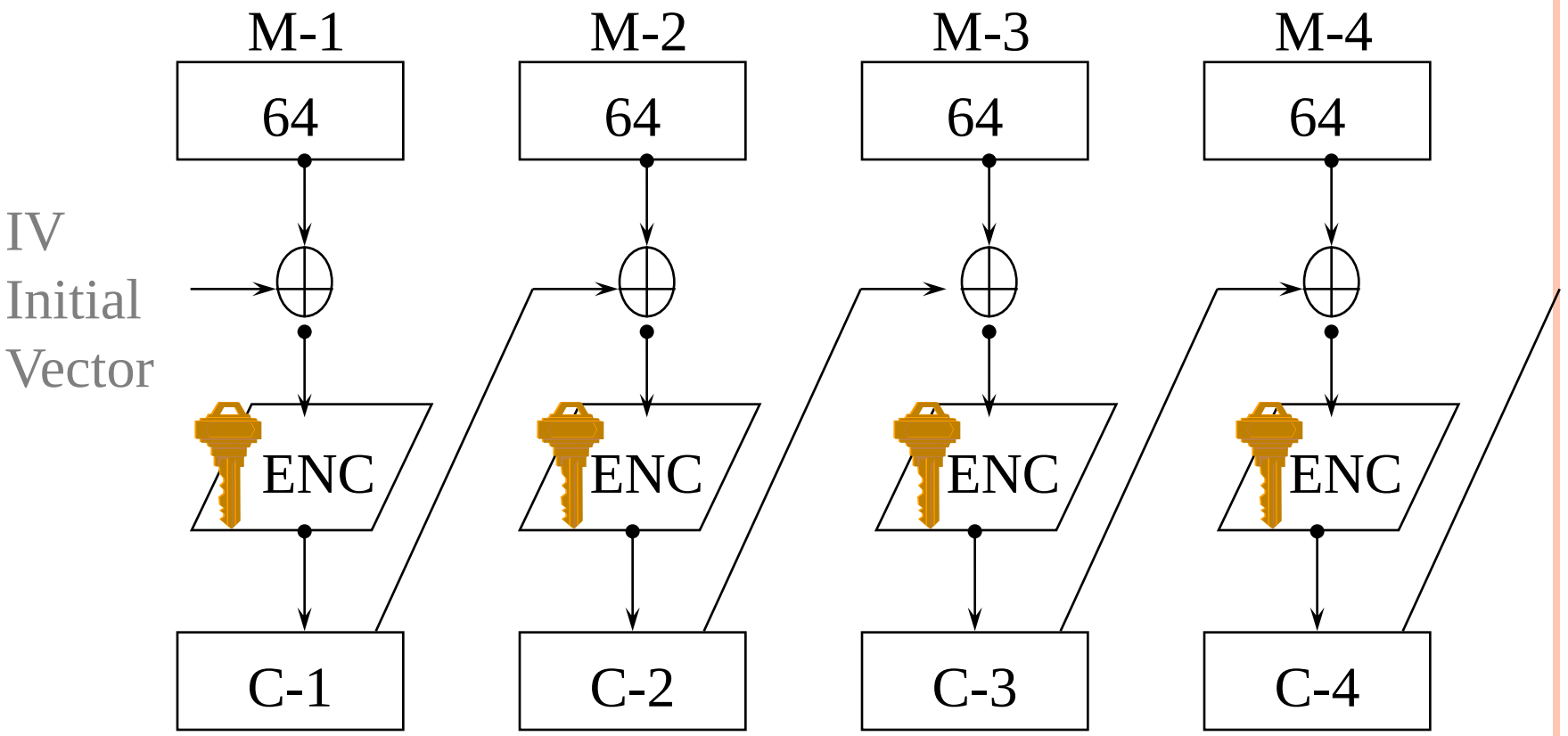
If we loss one C block, how many M blocks do we loss?

Will 64 bit IV make the key length (56+64) = 120 bits?

طول کلید با استفاده از IV بیشتر نمیشود

چون IV جزو استاندارد کاربری است و ثابت است

CBC Problems



1. Before ENC, we have one bit error in M-1!!
2. Sequential processing

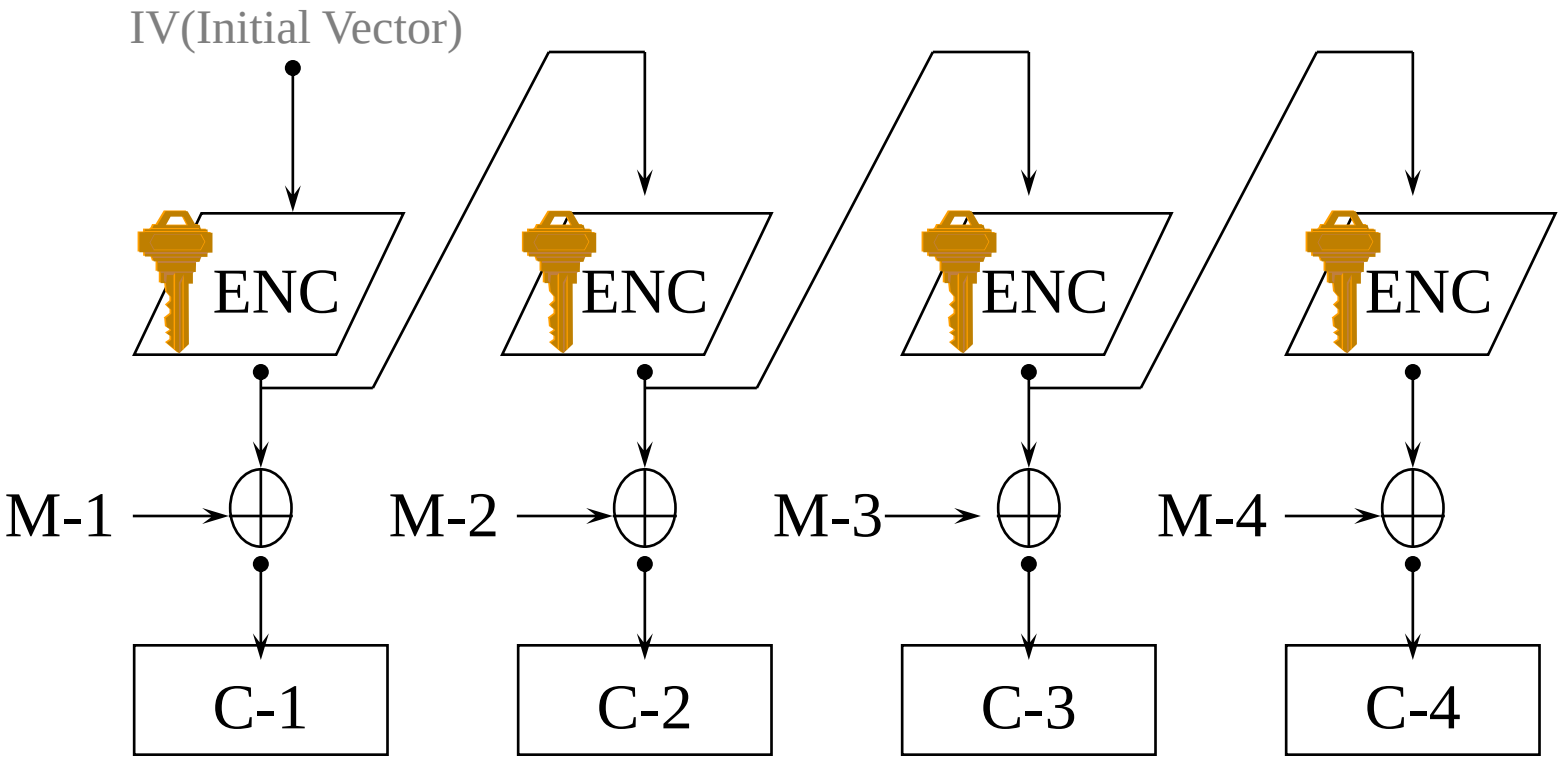
CBC Characteristic & Problems

- اگر در حین رمزنگاری بیتی از یک بلوک خراب شود روی بقیه فایل تاثیر نامطلوبی خواهد داشت و همه بلوک ها خراب خواهند شد
- اگر درمسیر ارسال داده رمز شده بیتی از بلوکی خراب شود روی همان بلوک و بلوک بعدی خود تاثیر خواهد داشت
- تاثیر پذیری کل خروجی رمز شده از بیت های قبلی به «انتشار رو به جلو» معروف است
- امکان موازی سازی در رمزنگاری وجود ندارد (رمز کردن P_i مستلزم رمز کردن P_{i-1}، P_{i-2} تا... P_0 است)

$$C_0 = E_k(P_0 \oplus IV)$$
$$C_i = E_k(P_i \oplus C_{i-1})$$

Output Feedback (OFB)

Random Number Generator.



OFB Characteristic & Problems

- برای *رمزنگاری*

$$C_i = P_i \oplus O_i$$

- برای *رمزگشایی*

$$P_i = C_i \oplus O_i$$

- تولید دنباله *اعداد تصادفی* (Keystream)

$$O_i = E_k(O_{i-1})$$
$$O_0 = IV$$

- خطا در این مدل منتشر نمی شود
- چون کلیدها زودتر تولید می شوند سرعت آن بالا است

OFB Characteristic & Problems

- حمله به این نوع رمزنگاری
- برای دو متن متفاوت P و Q اگر IV و k یکسان باشد دنباله اعداد تصادفی (Keystream) هر دو نیز یکسان خواهد بود :

$P : (P_0 \oplus K_0), (P_1 \oplus K_1), \ldots, (P_n \oplus K_n)$

$Q: (Q_0 \oplus K_0), (Q_1 \oplus K_1), \ldots, (Q_n \oplus K_n)$

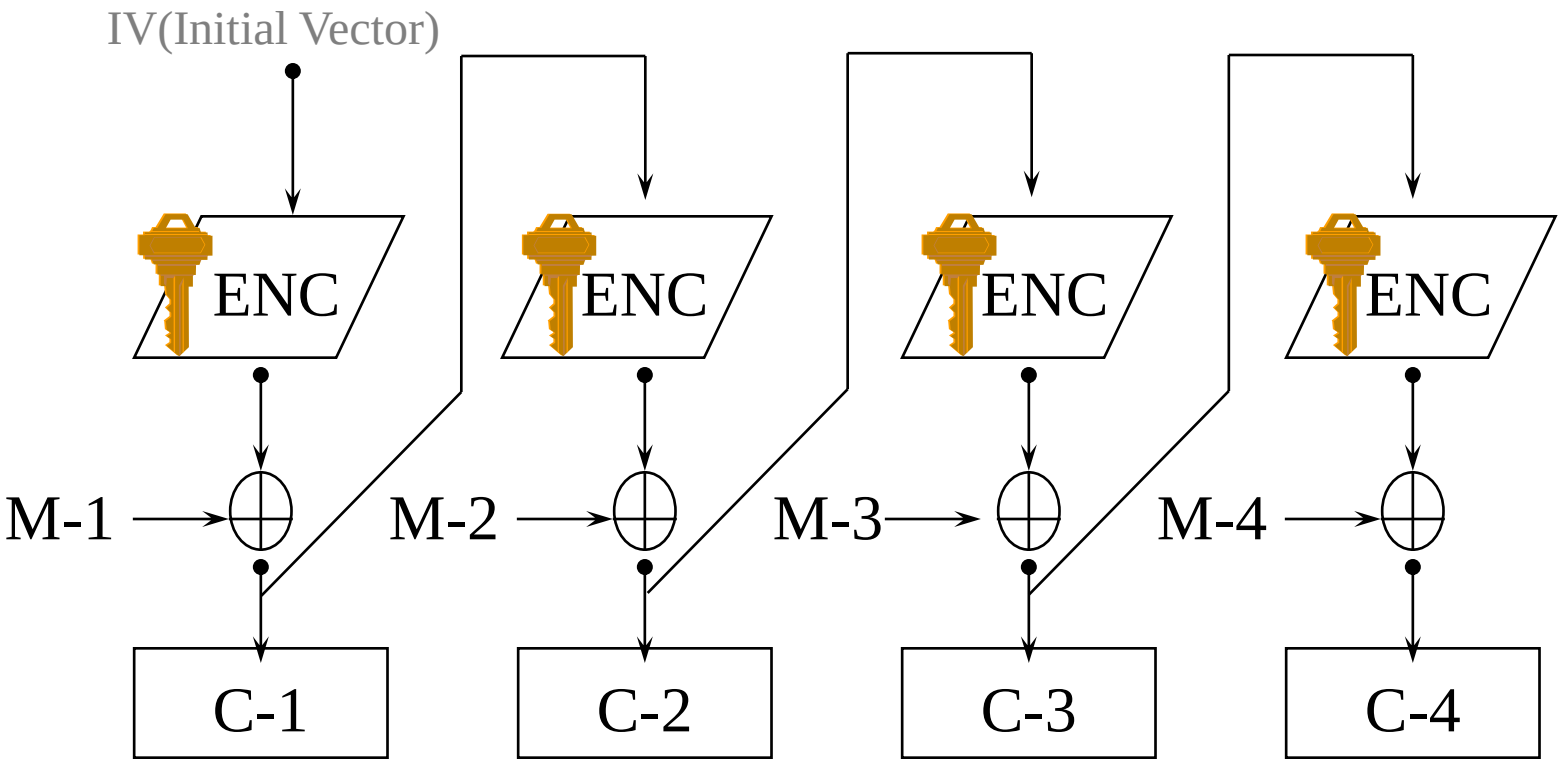
- اگر اخلال گر هر دو متن را استراق سمع کند :

$(P_i \oplus K_i) \oplus (Q_i \oplus K_i) = P_i \oplus Q_i$

- استفاده از ویژگی های آماری و حمله راحت تر

راه حل : IV متفاوت برای متون متفاوت

Cipher Feedback (CFB)



CFB Characteristic & Problems

- *برای رمزکردن*

$C_0 = IV$

$C_i = P_i \oplus E_k(C_{i-1})$

- بلوک متن هرگز وارد رمز کننده نمی شود
- *برای رمزگشایی*

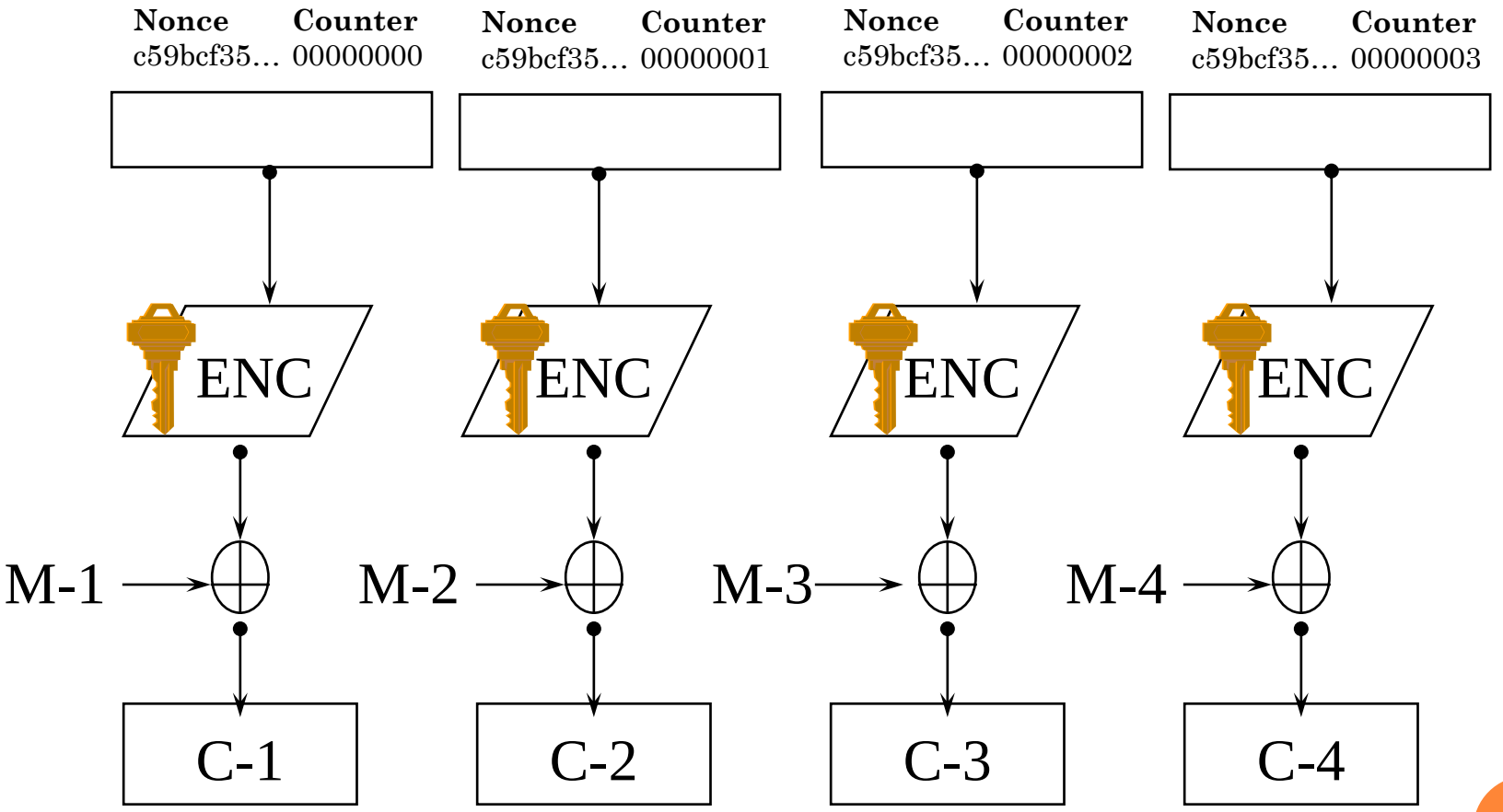
$C_0 = IV$

$P_i = C_i \oplus E_k(C_{i-1})$

- خطا در یک بیت از یک بلوک رمز شده کل متن را تحت تاثیر قرار خواهد داد
- برای رمزگشایی C_i فقط به $E_k(C_{i-1})$ نیاز است (با دریافت C_i رمزگشایی شروع می شود – pipelining)

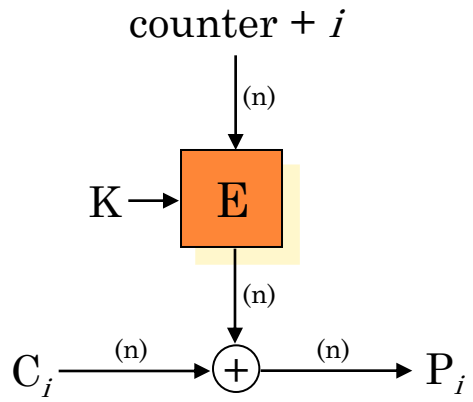
نکته : روش بهتر برای تاخیر کمتر، حالت *بلوکی* رمزنگار به حالت *بایتی* تغییر کند

Counter Mode (CTR)

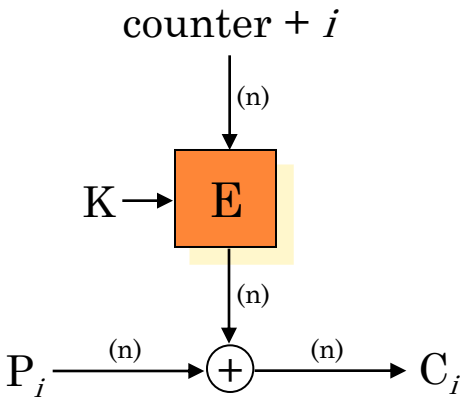


مد کاری CTR

- رمزگشایی ↓



- رمز نگاری ↓



بررسی مد کاری CTR

برای استفاده از رمزقطعه ای صرفا مقدار شمارنده موردنیاز است.
می توان ابتدا مقدار
$E_K(counter + i)$
C_i را محاسبه نمود و سپس با رسیدن متن نهایی را بازیابی کرد.

- ملزومات امنیتی:
  - مقادیر شمارنده، در بازه طول عمر کلید، باید مجزا باشند.
- رمزنگاری:
  - عملیات رمزنگاری قابل موازی سازی است.
  - برای عملیات رمزنگاری نیازی به متن واضح نیست.
  - مقادیر شمارنده برای عملیات رمزنگاری مورد نیاز است.
- رمزگشایی:
  - عملیات رمزگشایی قابل موازی سازی است.
  - برای عملیات رمزگشایی نیازی به متن رمز شده نیست.
  - مقادیر شمارنده برای عملیات رمزنگاری مورد نیاز است.
- طول پیام:
  - هیچ گاه نیازی به افزایش طول پیام نداریم.
    - متن رمز شده میتواند هم طول با پیام کوتاه شود.
- پیاده سازی:
  - تنها رمز نگاری باید پیاده سازی شود.

CTR Characteristic & Problems

- هیچ یک از سه روش قبلی برای رمز کردن فایل های بزرگ مناسب نیست
- بهترین شیوه برای دستیابی مستقیم به هر بلوک رمز «شیوه شمارنده – CTR» است
- وجود همان مشکل موجود در روش OFB، یعنی IV تکراری برای دو متن مجزا
- اگر متن بیش از اندازه طولانی باشد، احتمال برگشت شمارنده به ابتدا وجود دارد و بنابراین وجود خطر Keystream
- احتمال موفقیت حمله مشابه نگاری در یک نشست بسیار کم است چرا که فقط با رخداد شمارنده مشابه و متن ورودی مشابه در همان نشست امکانپذیر میشود که احتمال بسیار پایینی دارد،
- خوشبختانه در این روش امکان احصاء اطلاعات در یک نشست به منظور کاربری موثر و یا حمله مشابه نگاری در یک نشست دیگر بدلیل تفاوت nonce های متفاوت برای هرنشست وجود ندارد.

Counter Mode (CTR), Decryption