Securitatea Sistemelor Informatice

- Curs 6.1 -
Padding-oracle attack

Adela Georgescu

Facultatea de Matematică și Informatică
Universitatea din București
Anul universitar 2022-2023, semestrul I

Atacul bazat pe oracol de padding

- In cursul anterior am discutat despre securitate CCA

Atacul bazat pe oracol de padding

- In cursul anterior am discutat despre securitate CCA
- Motivăm importanța securității CCA arătând un atac devastator din viața reală

Atacul bazat pe oracol de padding

- In cursul anterior am discutat despre securitate CCA
- Motivăm importanța securității CCA arătând un atac devastator din viața reală
- Mai mult, atacul cere ca un adversar să poata afla numai dacă un text criptat modificat este unul valid (care se poate decripta corect), nefiind necesară întreaga funcționalitate a unui oracol de decriptare (care întoarce textul clar corespunzător unui text criptat).

Atacul bazat pe oracol de padding

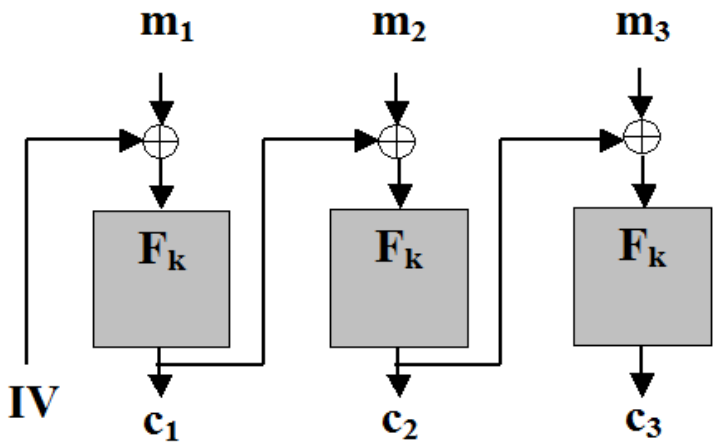
- In cursul anterior am discutat despre securitate CCA
- Motivăm importanța securității CCA arătând un atac devastator din viața reală
- Mai mult, atacul cere ca un adversar să poata afla numai dacă un text criptat modificat este unul valid (care se poate decripta corect), nefiind necesară întreaga funcționalitate a unui oracol de decriptare (care întoarce textul clar corespunzător unui text criptat).
- Acest fapt poate fi exploatat pentru aflarea întregului text clar

Atacul bazat pe oracol de padding

- Am văzut cum funcționeaza modul CBC când lungimea mesajului clar este multiplu de lungimea L blocului de criptat (suportat de F_k) in octeți

Atacul bazat pe oracol de padding

- Am văzut cum funcționeaza modul CBC când lungimea mesajului clar este multiplu de lungimea L blocului de criptat (suportat de F_k) in octeți



Decriptare

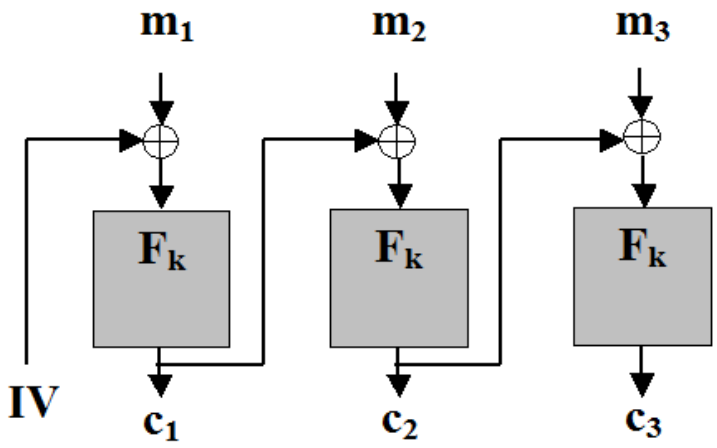
$$m_1 = \mathrm{F_k^{-1}}(c_1) \oplus \mathrm{IV}$$

$$m_2 = \mathrm{F_k^{-1}}(c_2) \oplus c_1$$

$$m_3 = \mathrm{F_k^{-1}}(c_3) \oplus c_2$$

Atacul bazat pe oracol de padding

- Am văzut cum funcționeaza modul CBC când lungimea mesajului clar este multiplu de lungimea L blocului de criptat (suportat de F_k) in octeți



Decriptare

$$m_1 = \mathrm{F_k^{-1}}(c_1) \oplus \mathrm{IV}$$

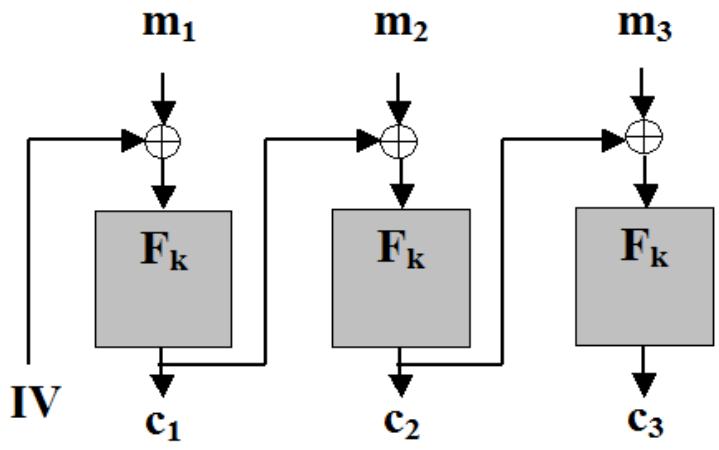
$$m_2 = \mathrm{F_k^{-1}}(c_2) \oplus c_1$$

$$m_3 = \mathrm{F_k^{-1}}(c_3) \oplus c_2$$

- Ce se întâmplă când $|m| \neq L$?

Atacul bazat pe oracol de padding

- Am văzut cum funcționeaza modul CBC când lungimea mesajului clar este multiplu de lungimea L blocului de criptat (suportat de F_k) in octeți



Decriptare

$$m_1 = \mathrm{F_k^{-1}}(c_1) \oplus \mathrm{IV}$$

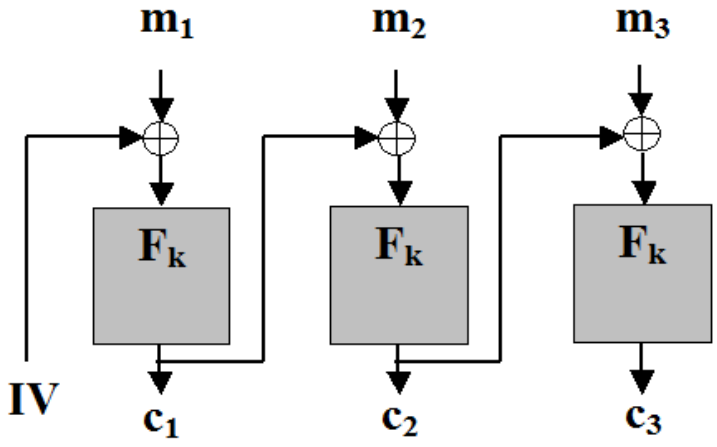
$$m_2 = \mathrm{F_k^{-1}}(c_2) \oplus c_1$$

$$m_3 = \mathrm{F_k^{-1}}(c_3) \oplus c_2$$

- Ce se întâmplă când $|m| \neq L$?
- Folosim padding-ul *PKCS#7* :
  - Fie b numărul de octeți de adăugat la ultimul bloc pentru a avea $|m|$ multiplu de L ($1 \leq b \leq L$)

Atacul bazat pe oracol de padding

- Am văzut cum funcționeaza modul CBC când lungimea mesajului clar este multiplu de lungimea L blocului de criptat (suportat de F_k) in octeți



Decriptare

$$m_1 = \mathrm{F_k^{-1}}(c_1) \oplus \mathrm{IV}$$

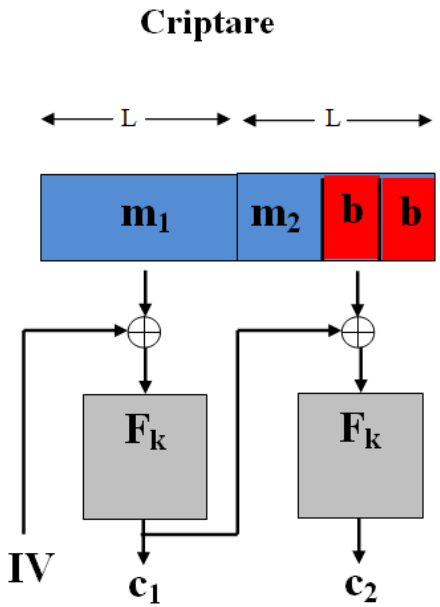
$$m_2 = \mathrm{F_k^{-1}}(c_2) \oplus c_1$$

$$m_3 = \mathrm{F_k^{-1}}(c_3) \oplus c_2$$

- Ce se întâmplă când $|m| \neq L$?
- Folosim padding-ul *PKCS#7* :
  - Fie b numărul de octeți de adăugat la ultimul bloc pentru a avea $|m|$ multiplu de L ($1 \leq b \leq L$)
  - Se adaugă b octeți la ultimul bloc din m, fiecare reprezentând valoarea lui b

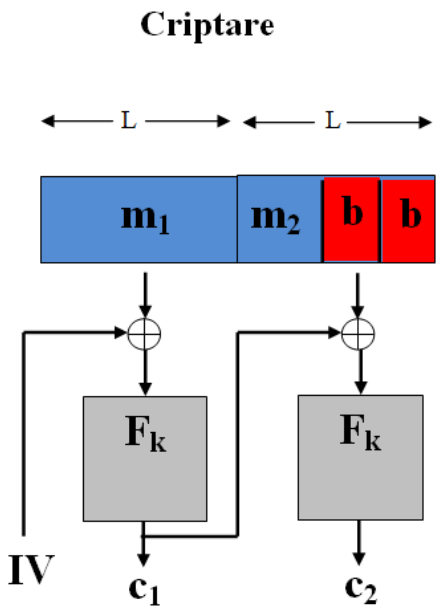
CBC cu padding PKCS7

Considerăm situația în care un client trimite mesaje criptate în modul CBC către un server.



CBC cu padding PKCS7

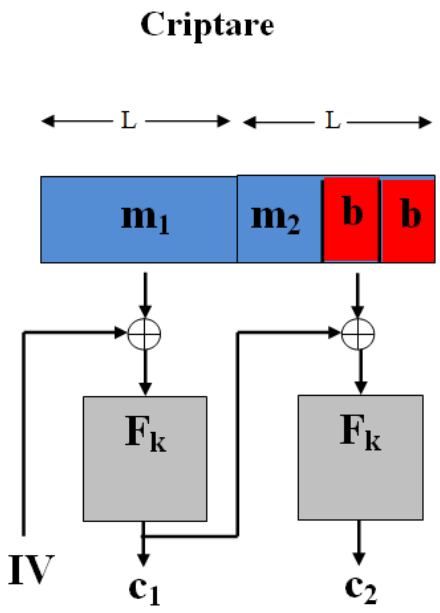
Considerăm situația în care un client trimite mesaje criptate în modul CBC către un server.



- în urma decriptării se obțin $m_1||m_2$

CBC cu padding PKCS7

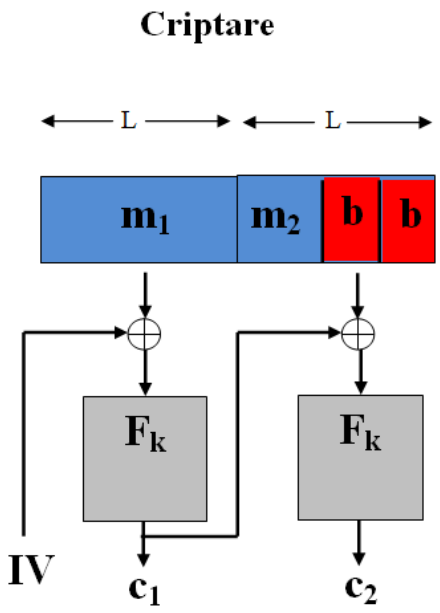
Considerăm situația în care un client trimite mesaje criptate în modul CBC către un server.



- în urma decriptării se obțin $m_1||m_2$
- se citește octetul final b

CBC cu padding PKCS7

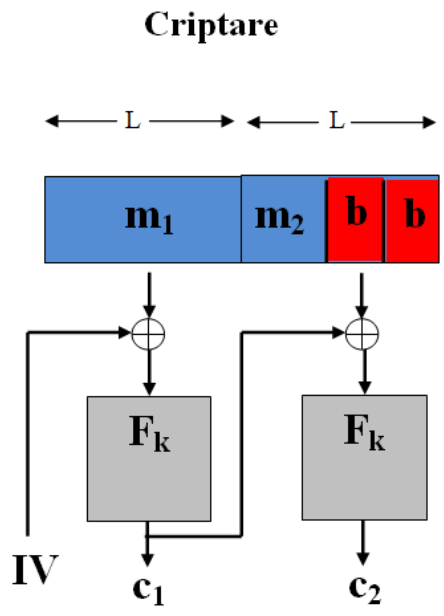
Considerăm situația în care un client trimite mesaje criptate în modul CBC către un server.



- în urma decriptării se obțin $m_1||m_2$
- se citește octetul final b
- dacă ultimii b octeți au toți valoarea b, atunci se scoate padding-ul și se obține mesajul original m

CBC cu padding PKCS7

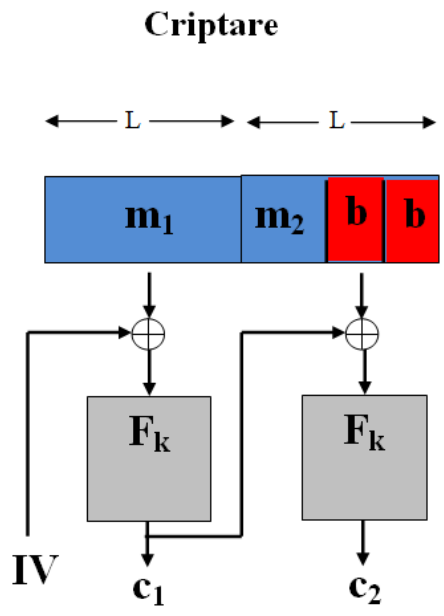
Considerăm situația în care un client trimite mesaje criptate în modul CBC către un server.



- în urma decriptării se obțin $m_1||m_2$
- se citește octetul final b
- dacă ultimii b octeți au toți valoarea b, atunci se scoate padding-ul și se obține mesajul original m
- altfel întoarce mesajul *padding gresit* și cere retransmiterea mesajului

CBC cu padding PKCS7

Considerăm situația în care un client trimite mesaje criptate în modul CBC către un server.



- în urma decriptării se obțin $m_1||m_2$
- se citește octetul final b
- dacă ultimii b octeți au toți valoarea b, atunci se scoate padding-ul și se obține mesajul original m
- altfel întoarce mesajul *padding gresit* și cere retransmiterea mesajului

Server-ul acționeaza ca un oracol de padding - adversarul îi trimite texte criptate și află dacă padding-ul este corect sau nu

Ideea atacului cu oracol de padding

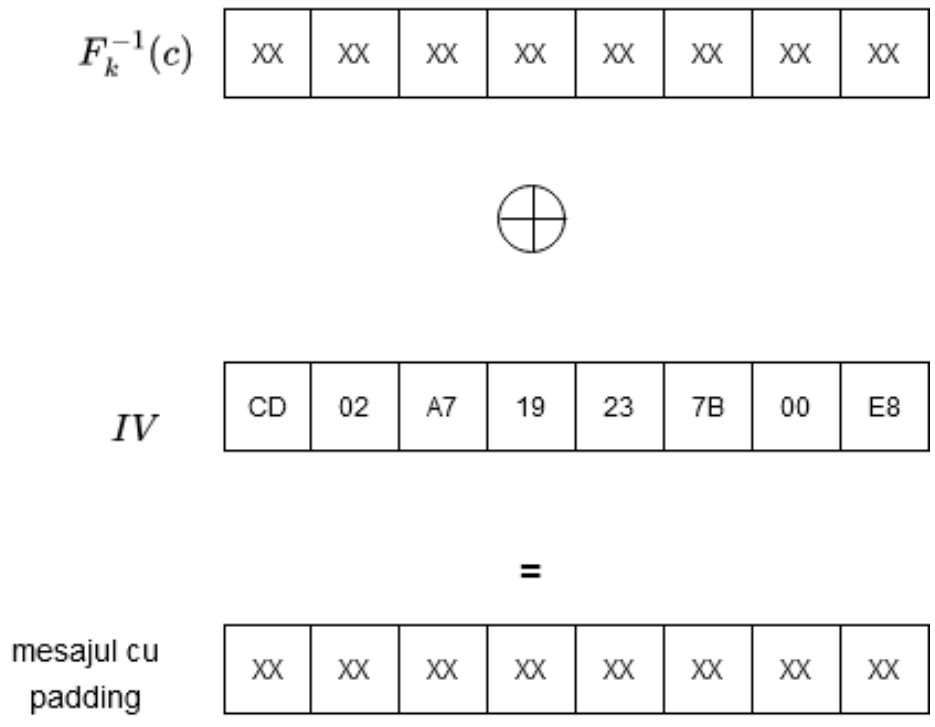
- Unui text criptat (IV, c) îi corespunde textul clar cu padding $m' = F_k^{-1}(c) \oplus IV$

Ideea atacului cu oracol de padding

- Unui text criptat (IV, c) îi corespunde textul clar cu padding $m' = F_k^{-1}(c) \oplus IV$
- Dacă un adversar modifică octetul i din IV atunci modificarea se va reflecta și în octetul i din m'

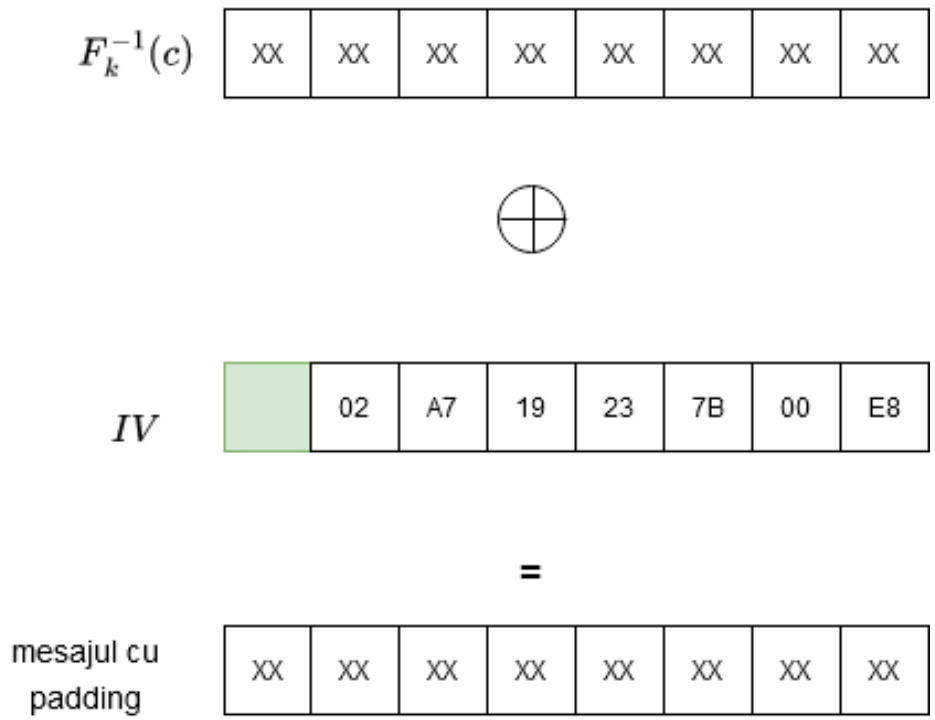
Ideea atacului cu oracol de padding

- Unui text criptat (IV, c) îi corespunde textul clar cu padding $m' = F_k^{-1}(c) \oplus IV$
- Dacă un adversar modifică octetul i din IV atunci modificarea se va reflecta și în octetul i din m'



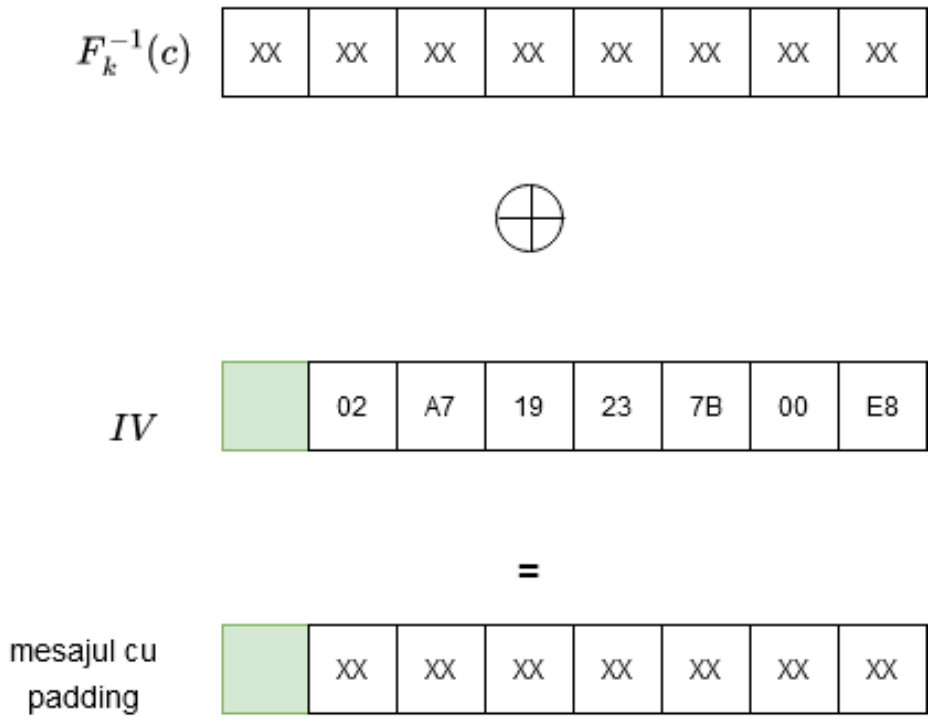
Ideea atacului cu oracol de padding

Adversarul modifica primul octet din IV



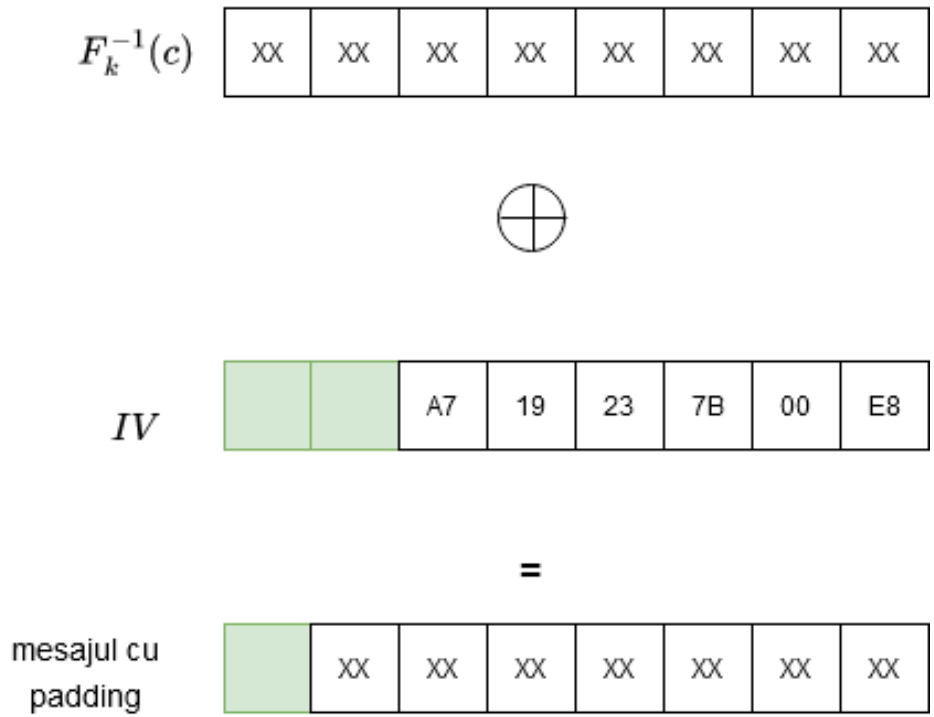
Ideea atacului cu oracol de padding

Modificarea se reflectă în primul octet din mesajul cu padding; apoi trimite mesajul (IV', c) și verifică dacă primește eroare



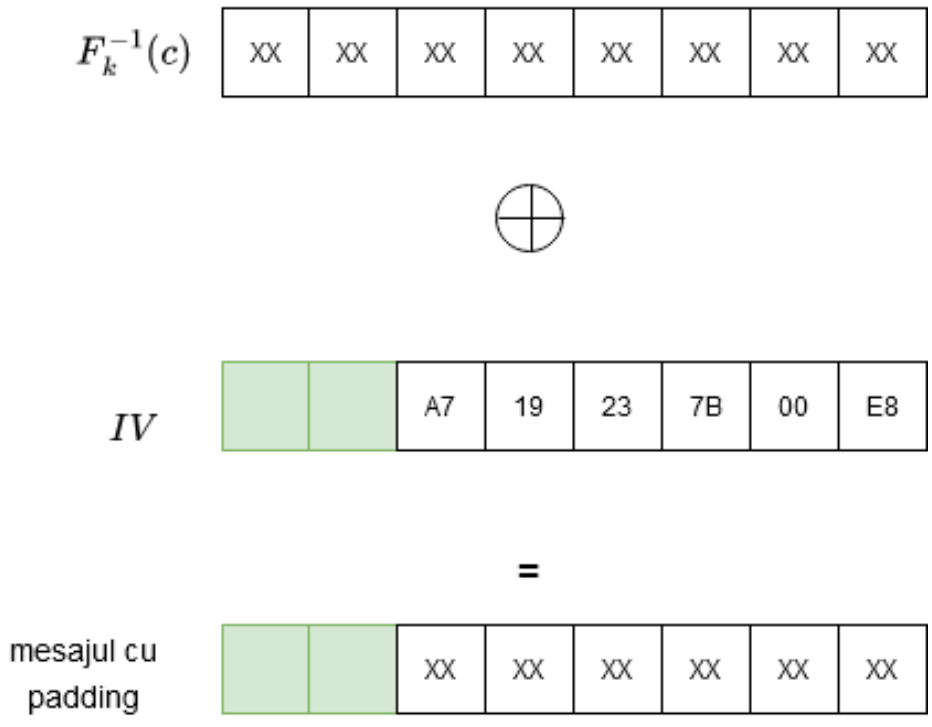
Ideea atacului cu oracol de padding

In caz contrar, adversarul modifică al 2-lea octet din IV



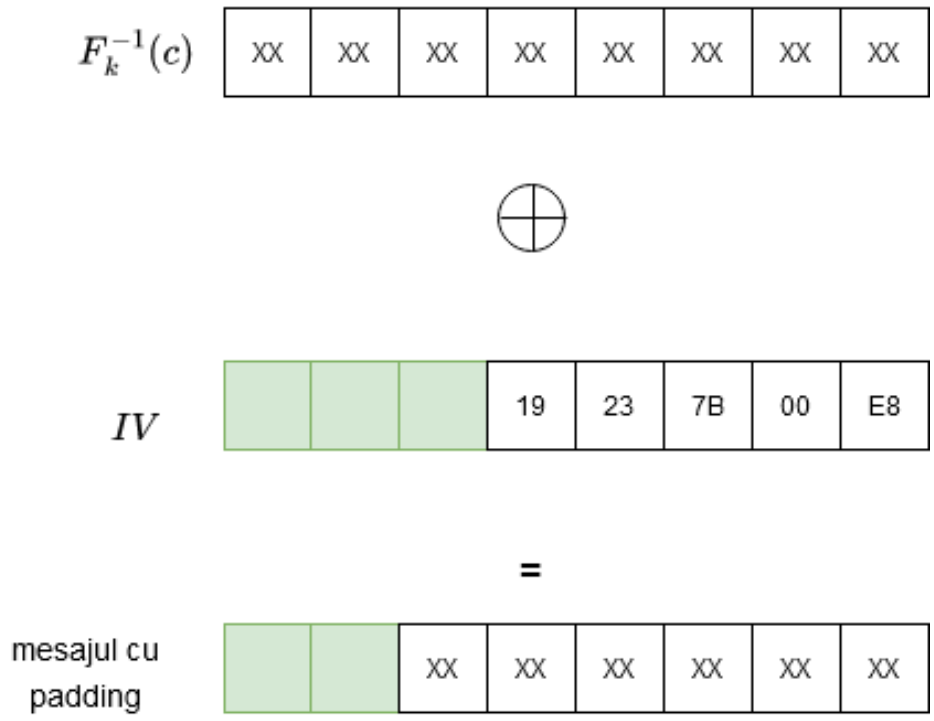
Ideea atacului cu oracol de padding

Modificarea se reflectă în al 2-lea octet din mesajul cu padding; apoi trimite mesajul (IV', c) și verifică dacă primește eroare

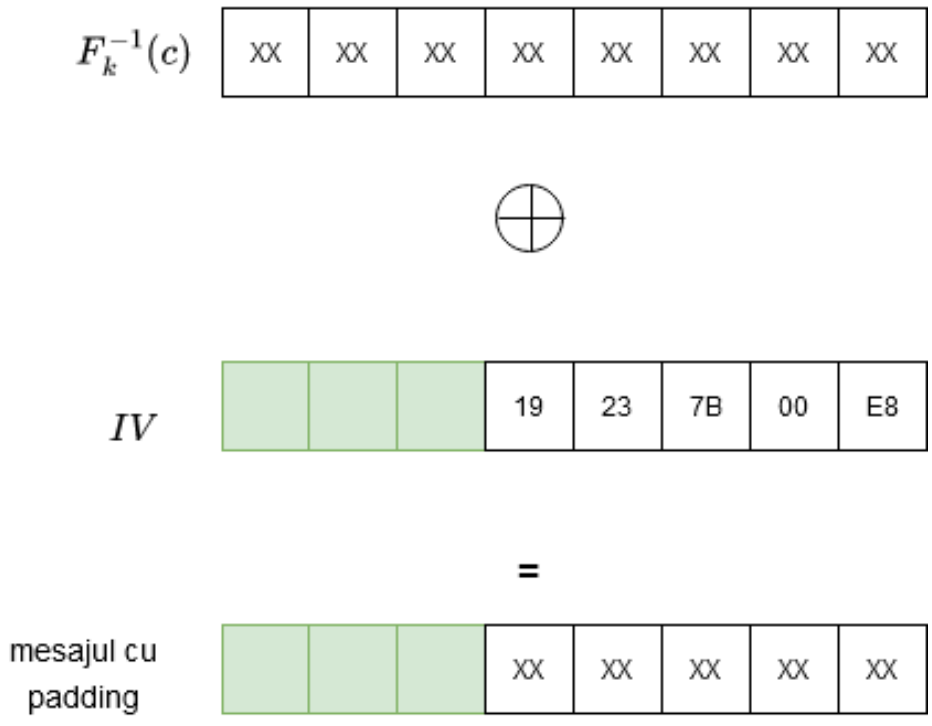


Ideea atacului cu oracol de padding

In caz contrar, adversarul continua cu al 3-lea octet din IV

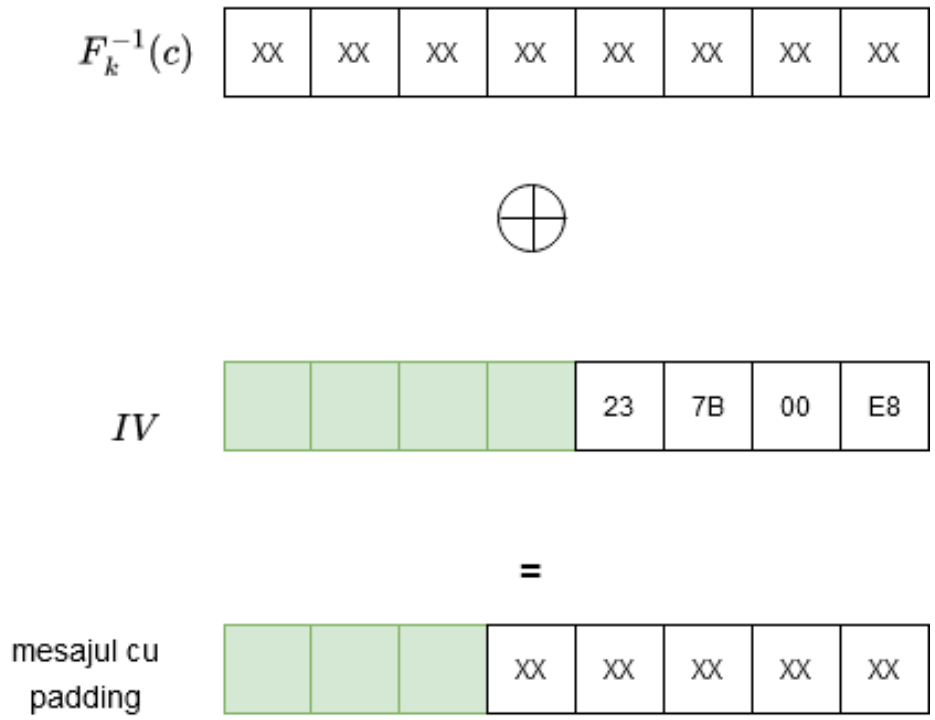


Ideea atacului cu oracol de padding

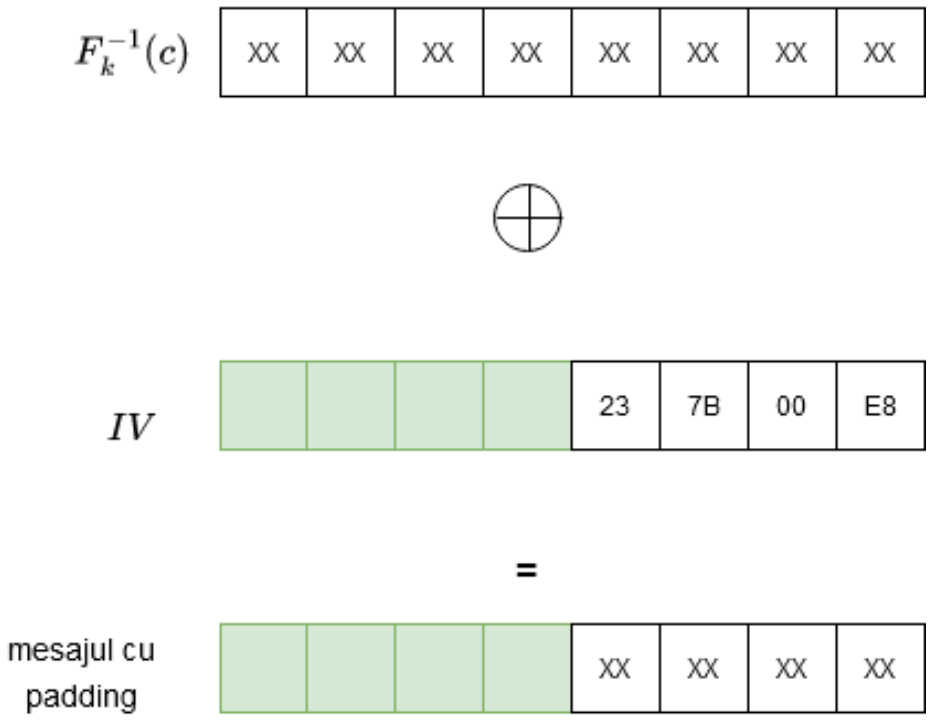


Ideea atacului cu oracol de padding

In caz contrar, adversarul continuă și cu al 4-lea octet din IV

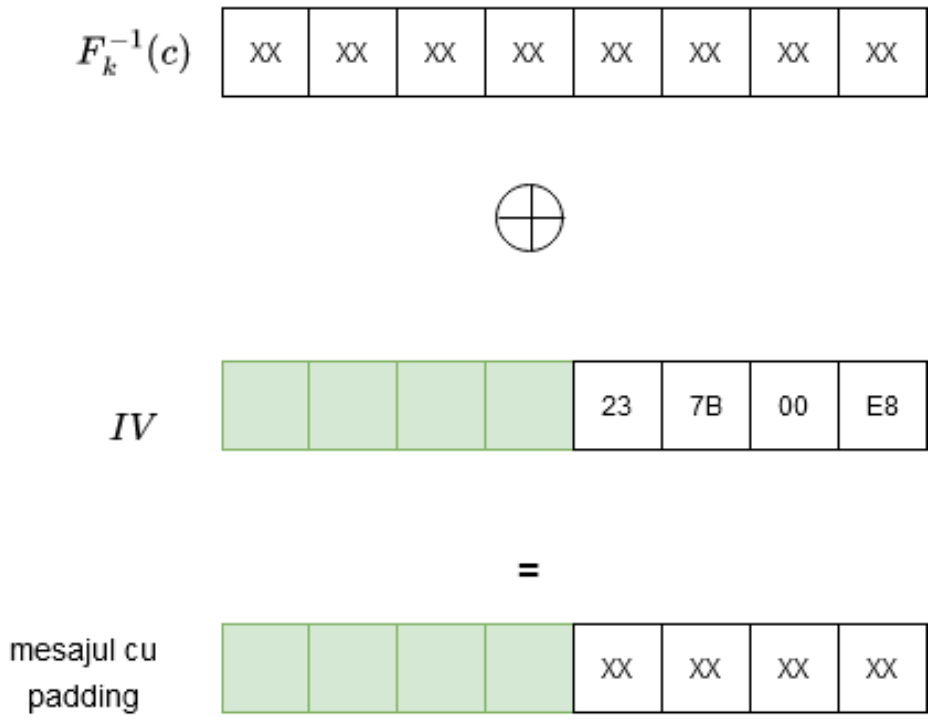


Ideea atacului cu oracol de padding



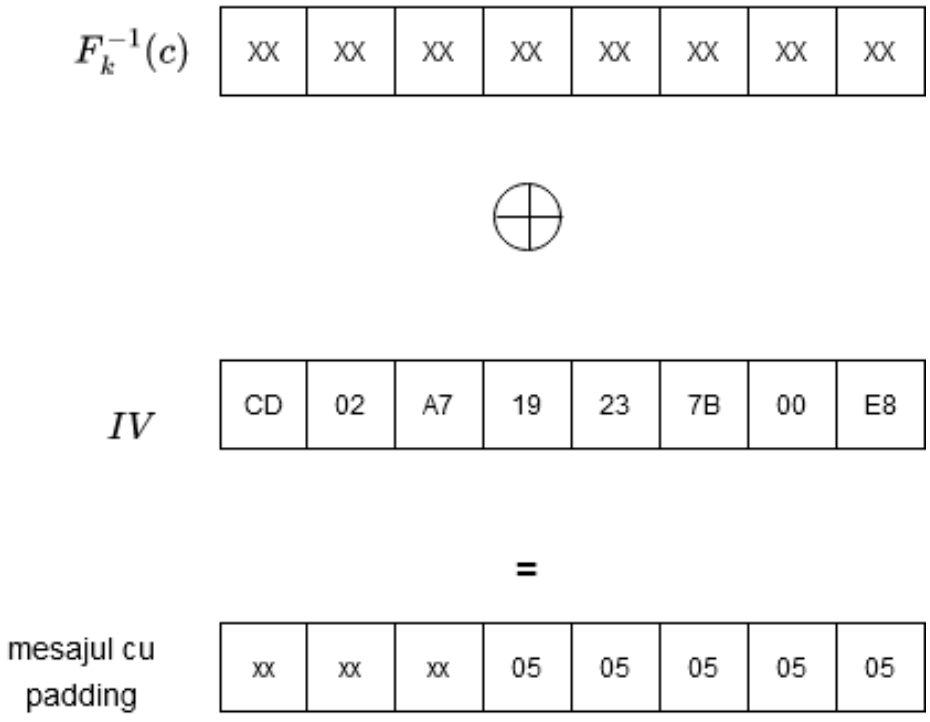
- Eroare la decriptare

Ideea atacului cu oracol de padding

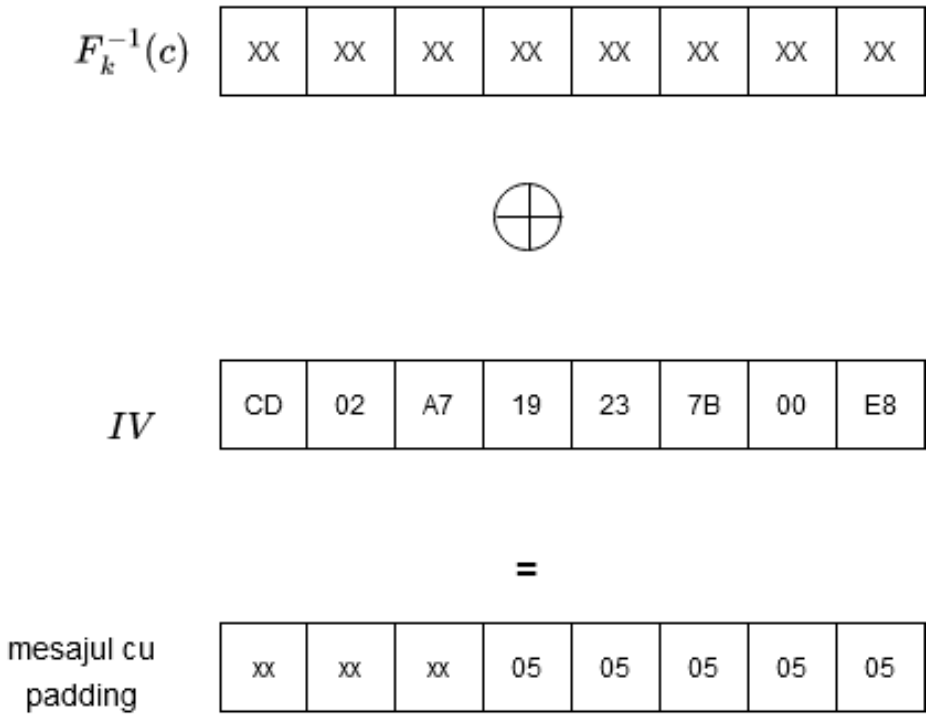


- Eroare la decriptare
- adversarul deduce ca oracolul verifica ultimii 5 octeti, care au valoarea 05

Ideea atacului cu oracol de padding



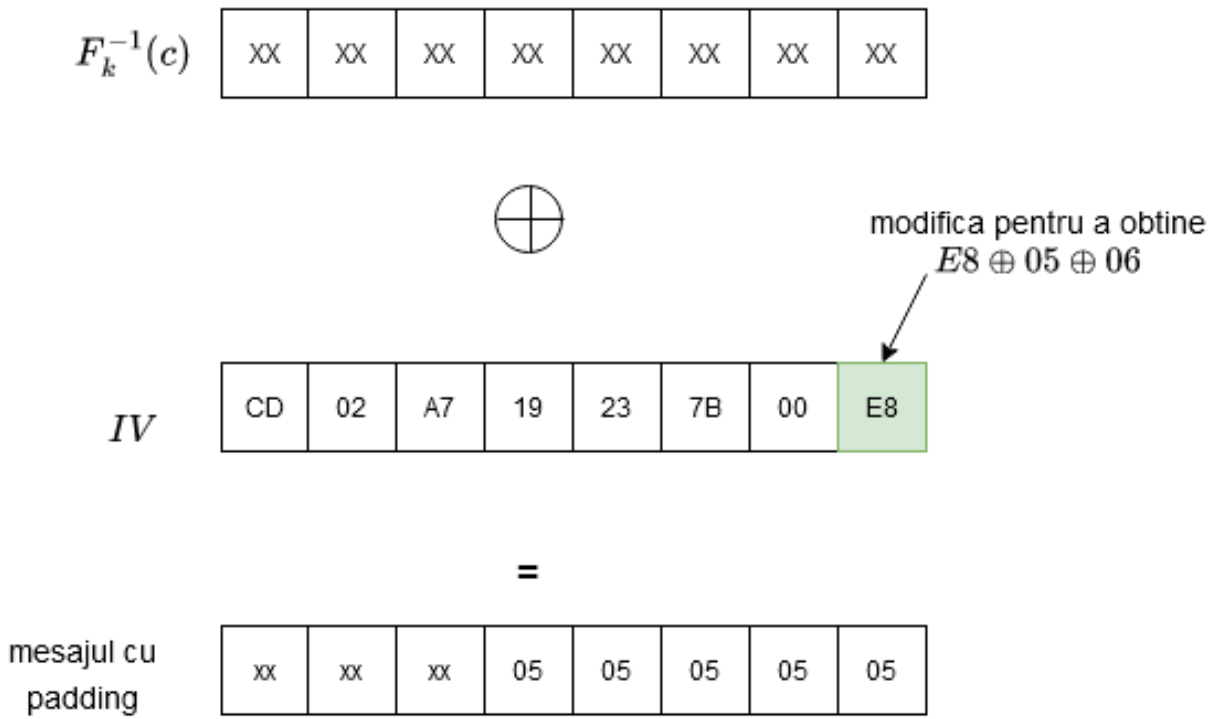
Ideea atacului cu oracol de padding



Primii 3 octeti din mesajul cu padding sunt încă necunoscuți atacatorului

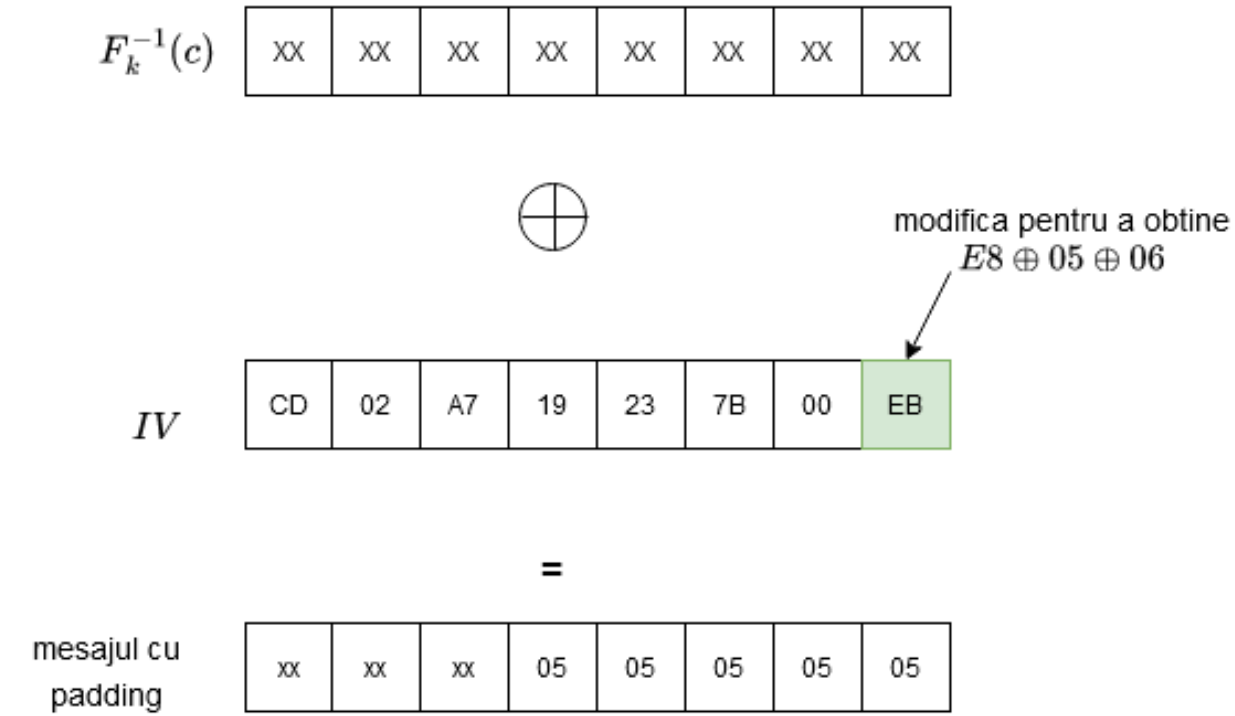
Ideea atacului cu oracol de padding

Adversarul încearcă să găsească primii 3 octeți din mesajul cu padding



Ideea atacului cu oracol de padding

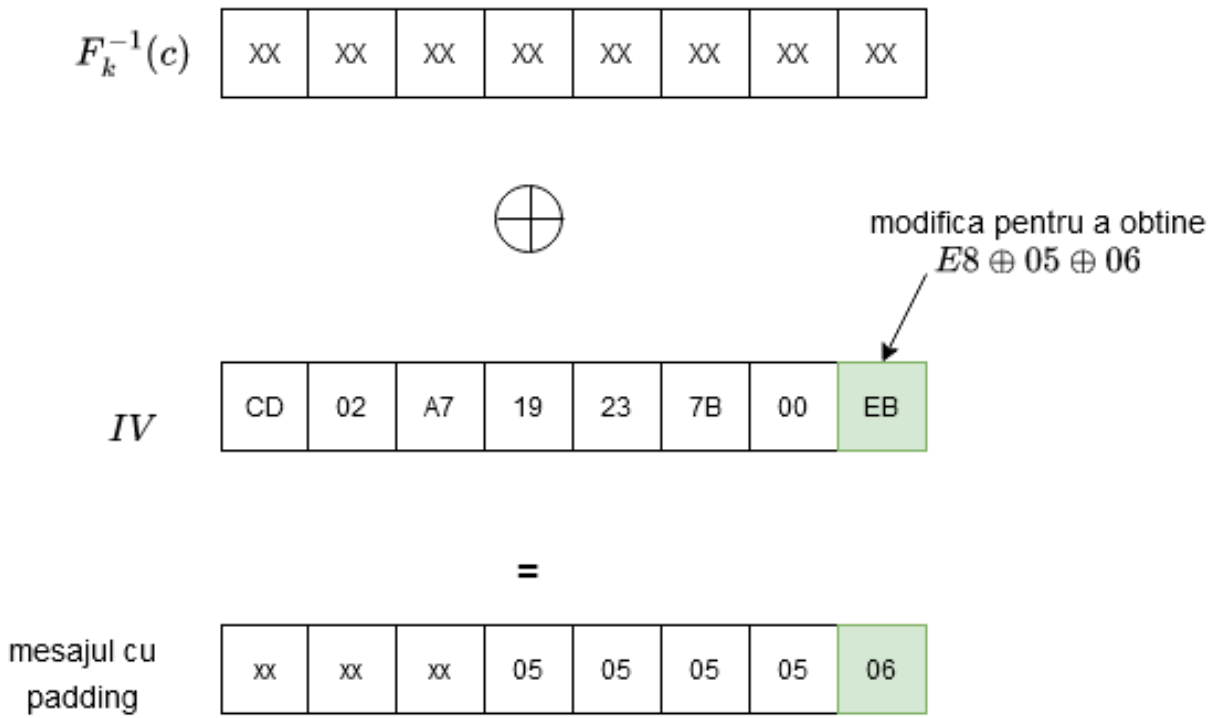
Adversarul încearcă să găsească primii 3 octeți din mesajul cu padding
El modifica cel mai din dreapta octet din IV



Ideea atacului cu oracol de padding

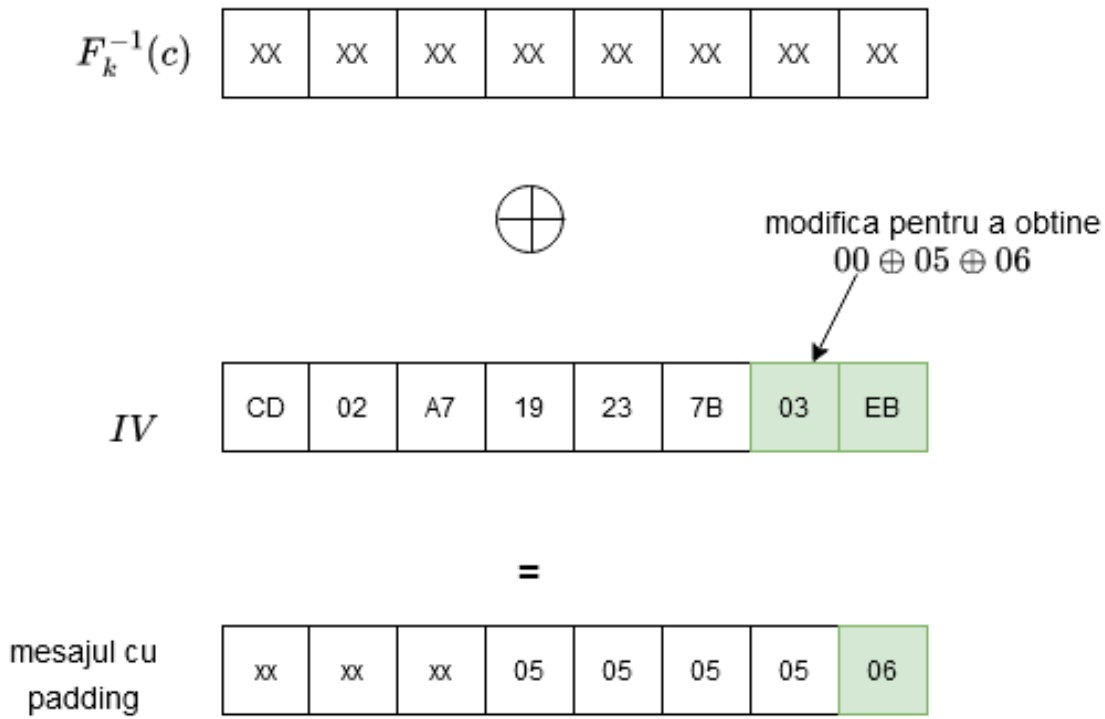
Adversarul încearcă să găsească primii 3 octeți din mesajul cu padding

Modificarea se va reflecta in cel mai din dreapta octet din mesajul cu padding

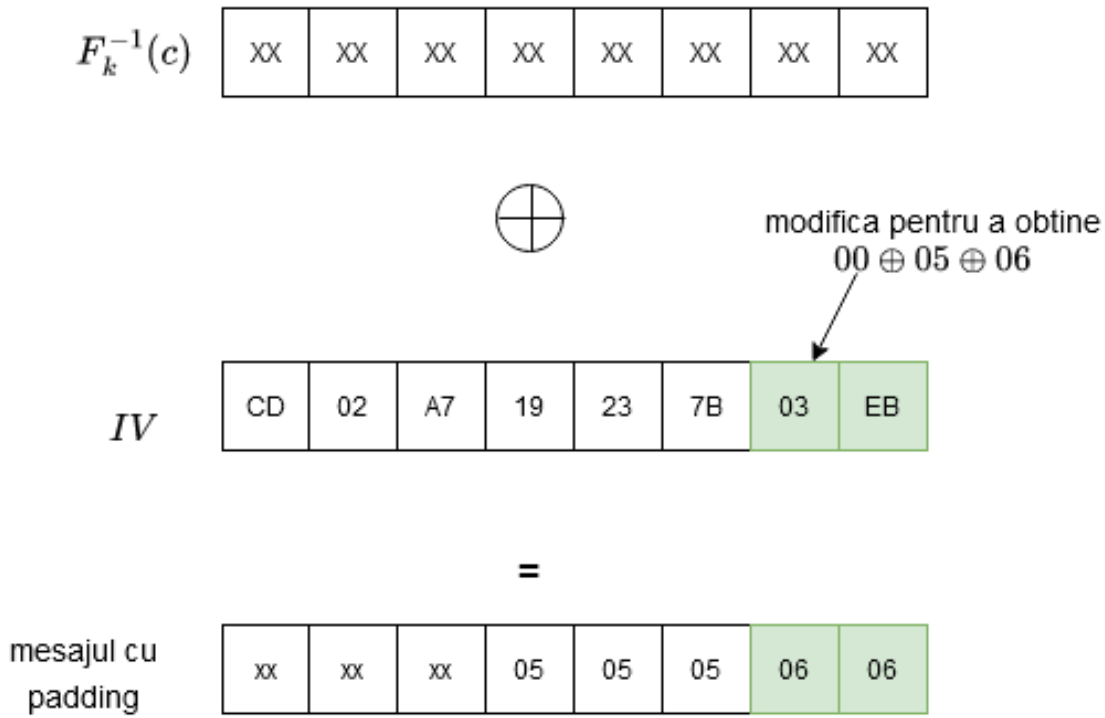


Ideea atacului cu oracol de padding

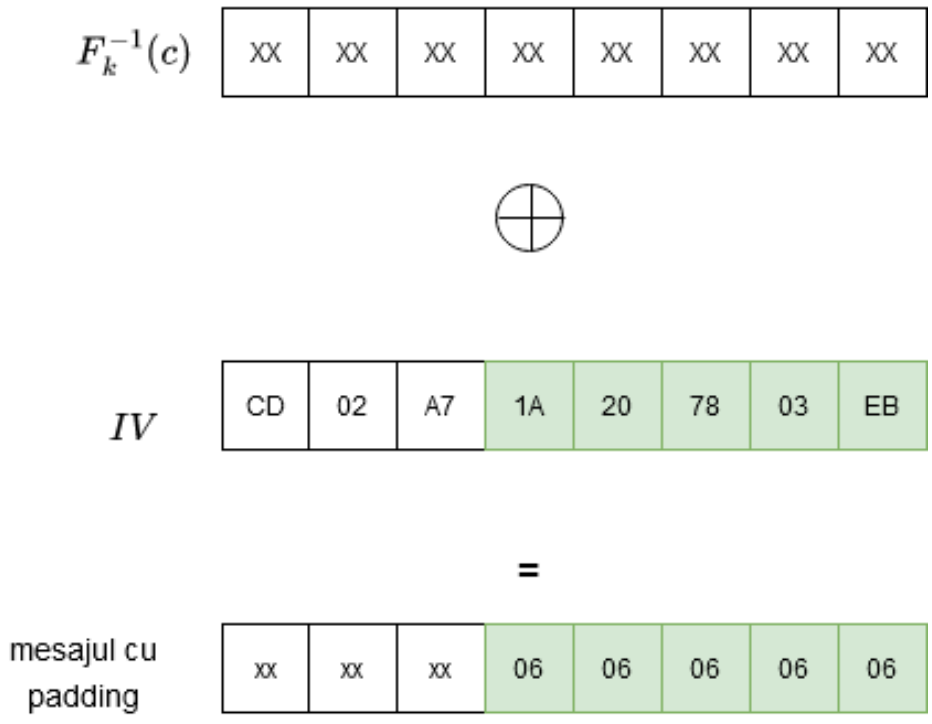
Adversarul va proceda similar pentru ceilalti octeti



Ideea atacului cu oracol de padding

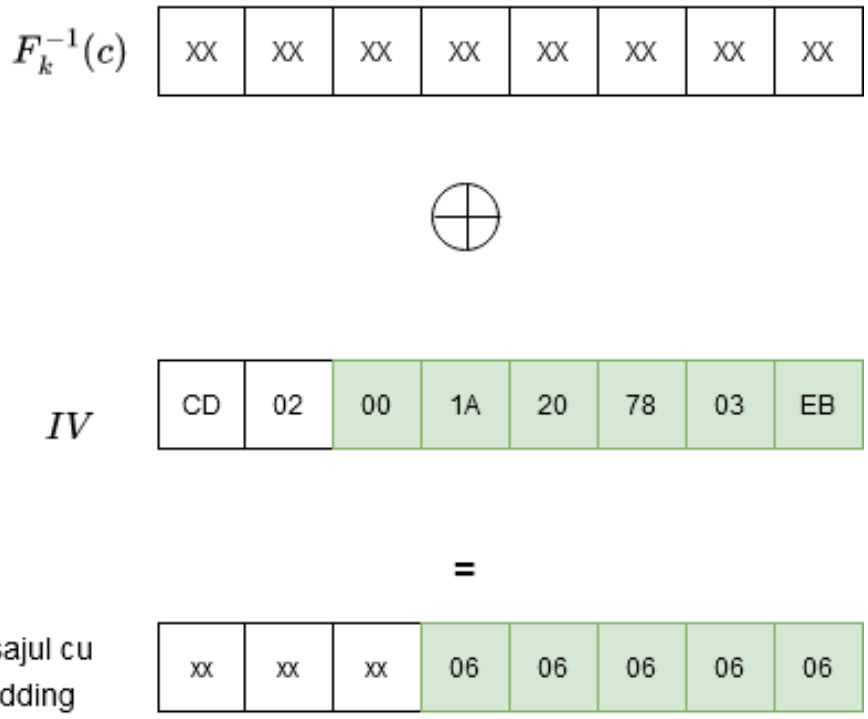


Ideea atacului cu oracol de padding



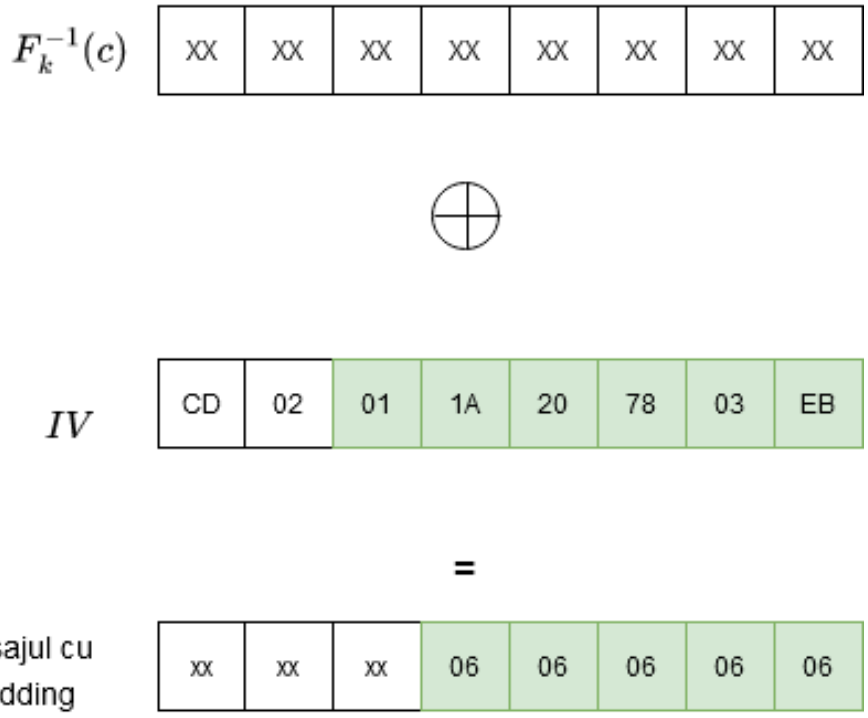
Dacă adversarul trimite acest IV împreună cu c, sunt șanse mici să nu primească eroare la decriptare

Ideea atacului cu oracol de padding



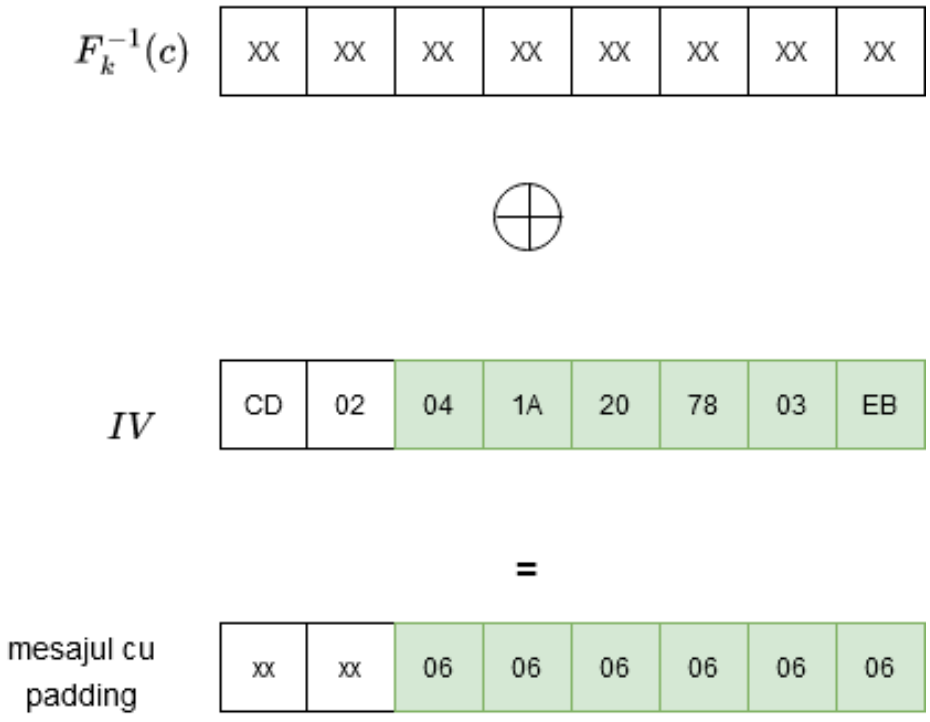
Va incerca pe rand toate valorile posibile pentru al 3-lea octet din IV ....

Ideea atacului cu oracol de padding



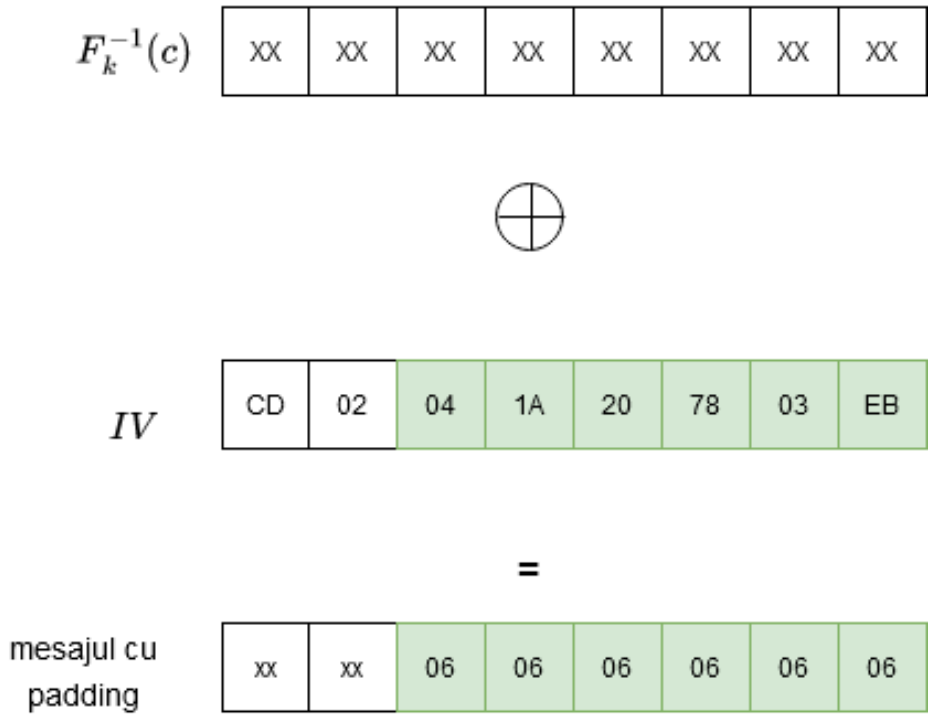
Va încerca pe rând toate valorile posibile pentru al 3-lea octet din IV ....

Ideea atacului cu oracol de padding



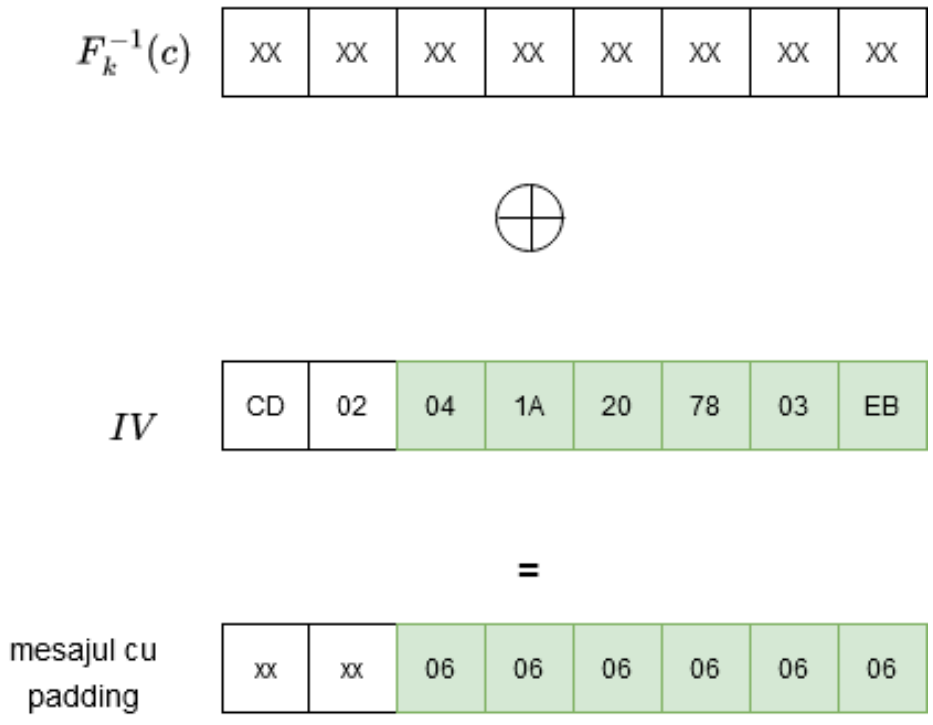
Până cand decriptarea va funcționa; când aceasta se întâmplă, al 3-lea octet din mesajul cu padding este 06 (doar atunci decriptarea funcționează)

Ideea atacului cu oracol de padding



Acum A cunoaște $xx \oplus 04 = 06$ și deci el poate calcula $xx \oplus A7$ (valoarea inițială a mesajului cu padding pe octetul 3).

Ideea atacului cu oracol de padding



Adversarul poate repeta același proces pentru a afla al doilea octet și apoi primul din mesajul cu padding.

Complexitatea atacului cu oracol de padding

- sunt necesare cel mult L incercări pentru a afla b

Complexitatea atacului cu oracol de padding

- sunt necesare cel mult L incercări pentru a afla b
- cel mult $2^8 = 256$ încercări pentru a afla fiecare octet din mesajul inițial

Complexitatea atacului cu oracol de padding

- sunt necesare cel mult L incercări pentru a afla b
- cel mult $2^8 = 256$ încercări pentru a afla fiecare octet din mesajul inițial
- în total sunt necesare 256 * *bt* încercări (unde *bt* reprezintă numărul de octeți din mesajul original) pentru a găsi întregul text clar