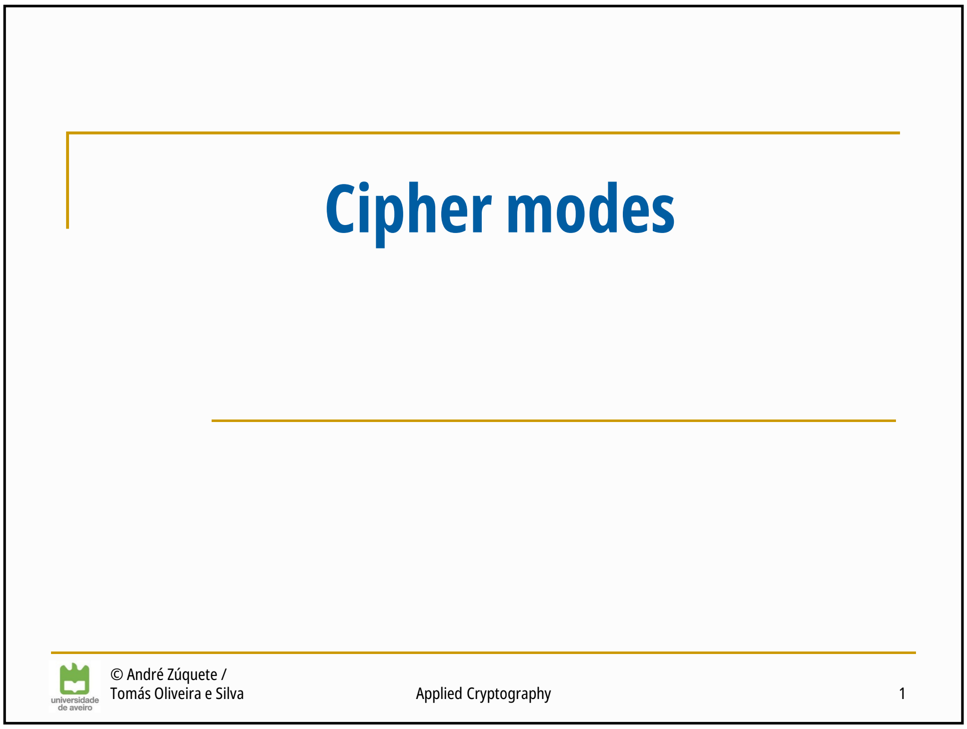
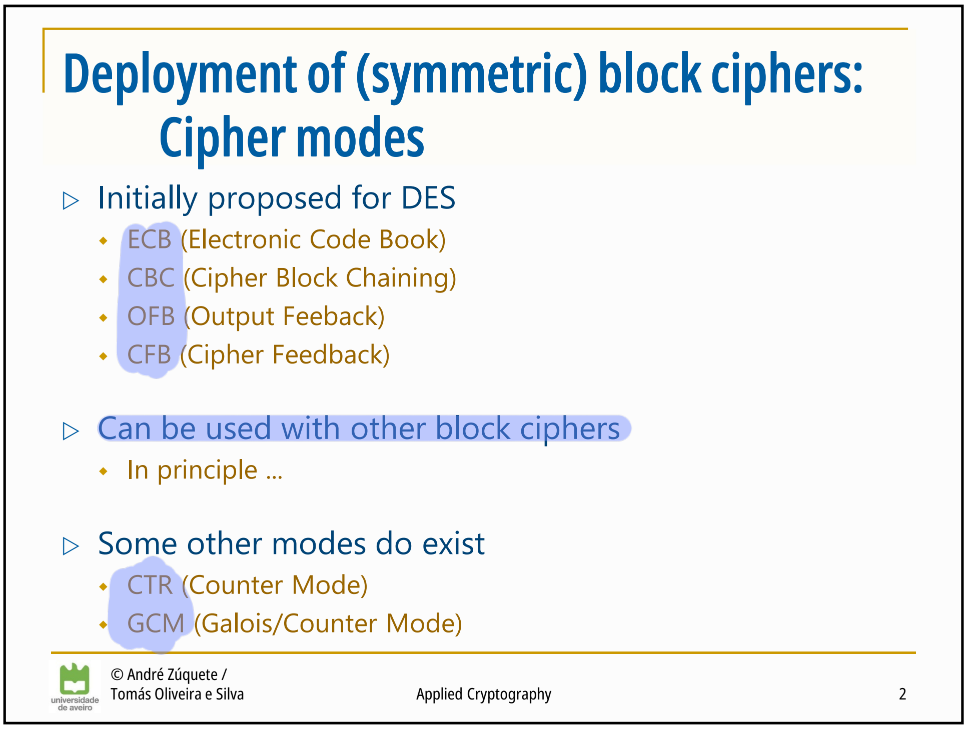


Cipher modes



Deployment of (symmetric) block ciphers: Cipher modes

- ▷ Initially proposed for DES
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - OFB (Output Feeback)
  - CFB (Cipher Feedback)
- ▷ Can be used with other block ciphers
  - In principle …
- ▷ Some other modes do exist
  - CTR (Counter Mode)
  - GCM (Galois/Counter Mode)

Block cipher modes: ECB and CBC

→ Cannot enc. in paralel
Can dec. in paralel

Electronic Code Book

$C_i = E_K(T_i)$

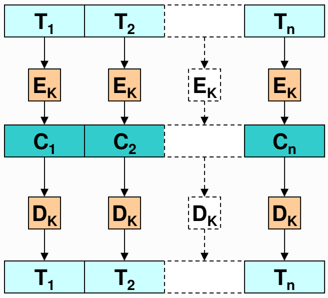
$T_i = D_K(C_i)$

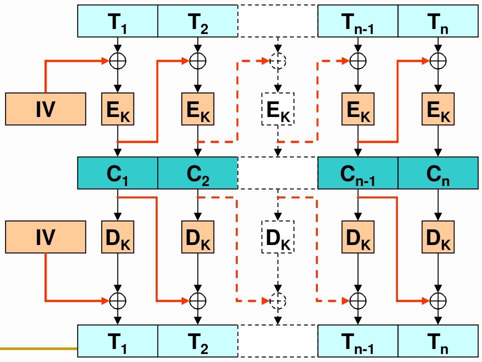
is monoalfabetic

Cipher Block Chaining

$C_i = E_K(T_i \oplus C_{i-1})$

$T_i = D_K(C_i) \oplus C_{i-1}$





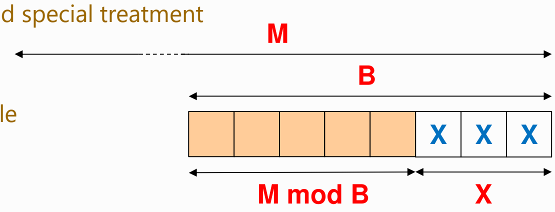
you have Uniform Random Access

ECB/CBC cipher modes: Block alignment with padding

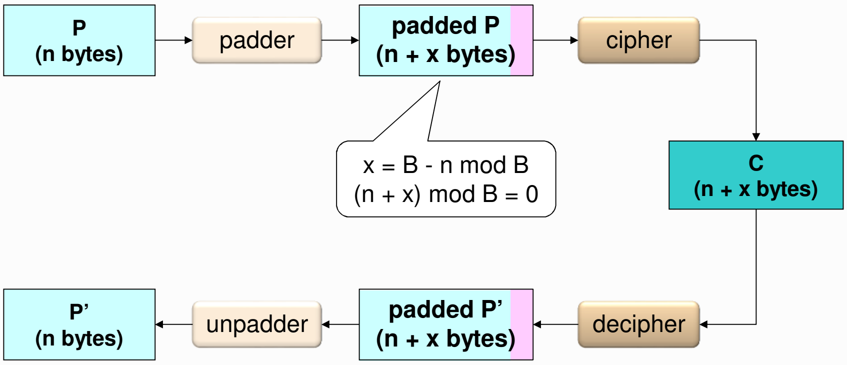
- ▷ Block cipher modes ECB and CBC require block-aligned inputs
  - Trailing sub-blocks need special treatment
- ▷ Alternative 1: padding
  - Of last block, identifiable
  - Adds data
  - PKCS #7
    - X = B – (M mod B)
    - X extra bytes, with the value X
    - PKCS #5 (same as PKCS #7 with B = 8)

is any value of B

- ▷ Alternative 2: different processing for the last block
  - Adds implementation complexity

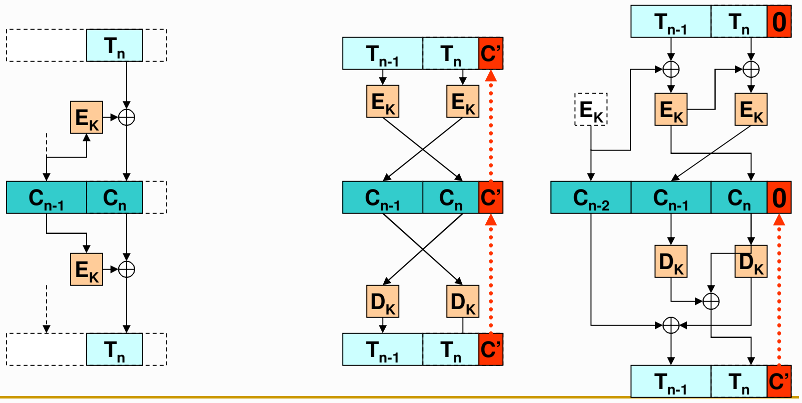


Padded block encryption / decryption



ECB/CBC cipher modes: Handling trailing sub-blocks

- ▷ Sort of stream cipher
- ▷ Ciphertext stealing



Curiosity not important

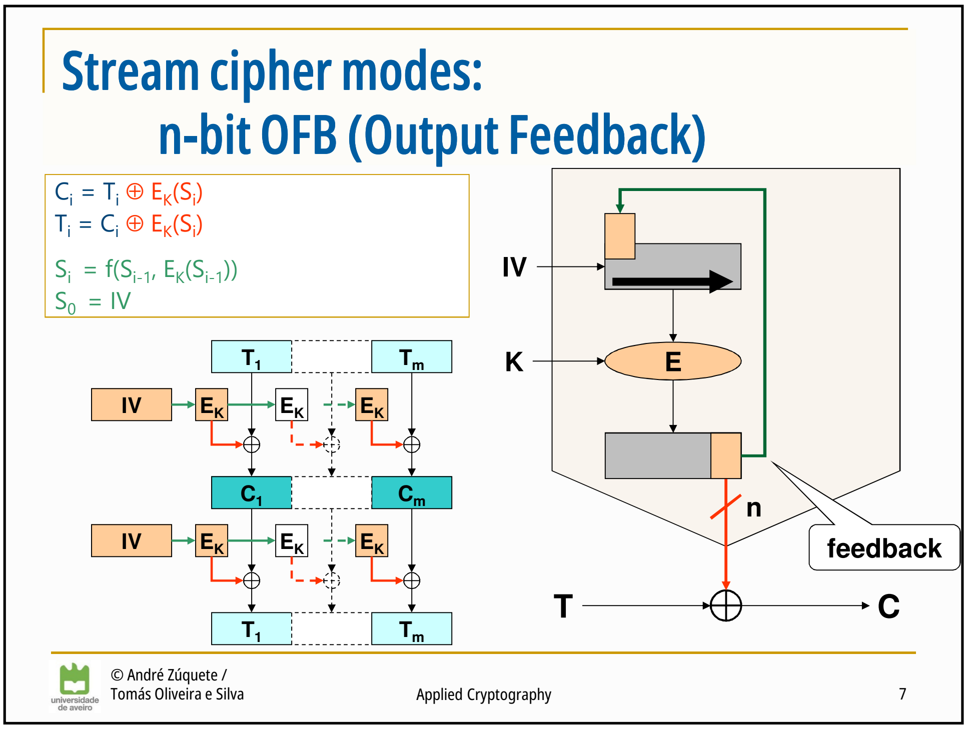
OFB não se sabe quando

stateo

Dmos acaba por entre em

ciclos

o estado inicial muda sempre, por causa do iv



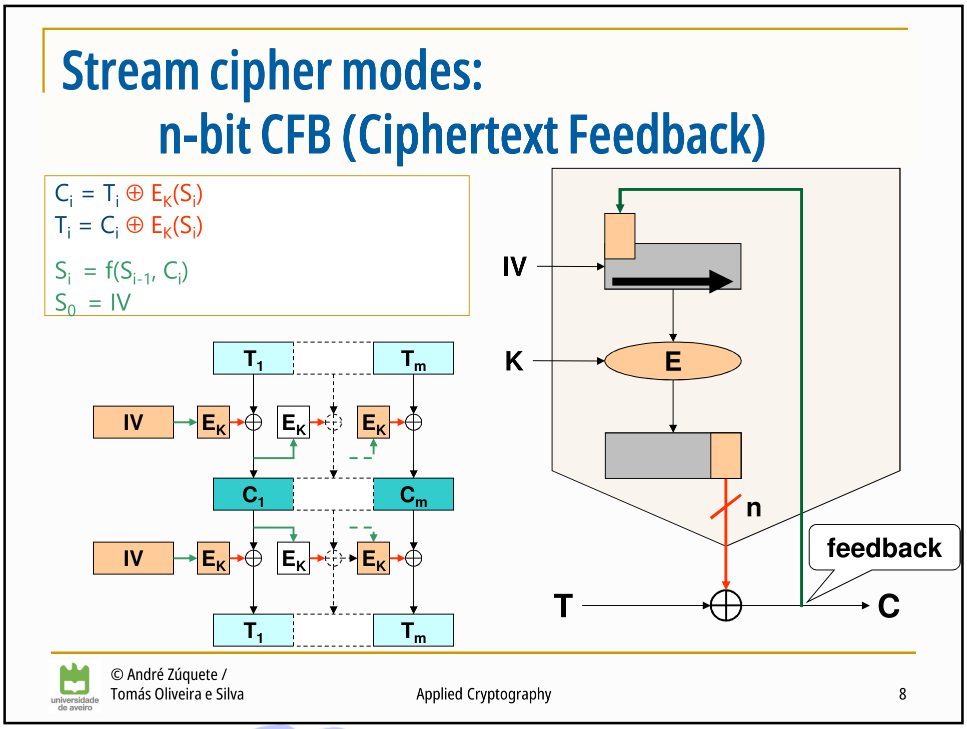
Stream cipher modes: n-bit OFB (Output Feedback)

$C_i = T_i \oplus E_K(S_i)$
$T_i = C_i \oplus E_K(S_i)$

$S_i = f(S_{i-1}, E_K(S_{i-1}))$
$S_0 = IV$

wifi-uses → AES CCMP

IV don't repeat it !!!! Never, because it makes the same Text



Stream cipher modes: n-bit CFB (Ciphertext Feedback)

$C_i = T_i \oplus E_K(S_i)$
$T_i = C_i \oplus E_K(S_i)$

$S_i = f(S_{i-1}, C_i)$
$S_0 = IV$

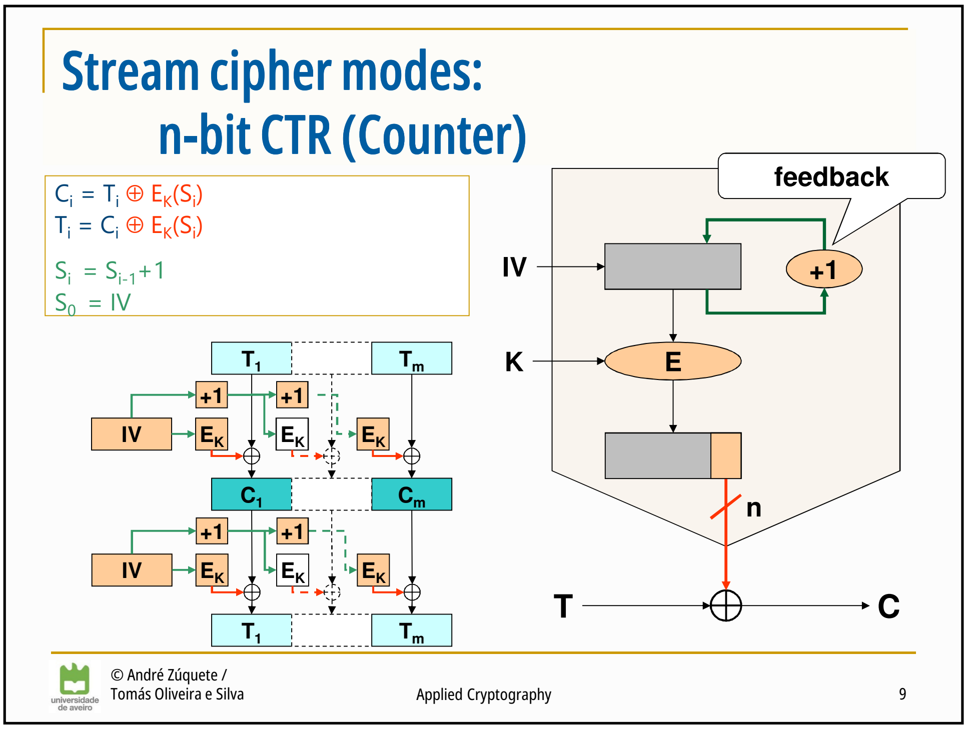
Doesn't cycle !!

IF you losse some data of enc. in transmition the cypher still works, self synchronization

Unless in most cases:

Useless

uniform Random Acess in decription only



Stream cipher modes: n-bit CTR (Counter)

$C_i = T_i \oplus E_K(S_i)$
$T_i = C_i \oplus E_K(S_i)$

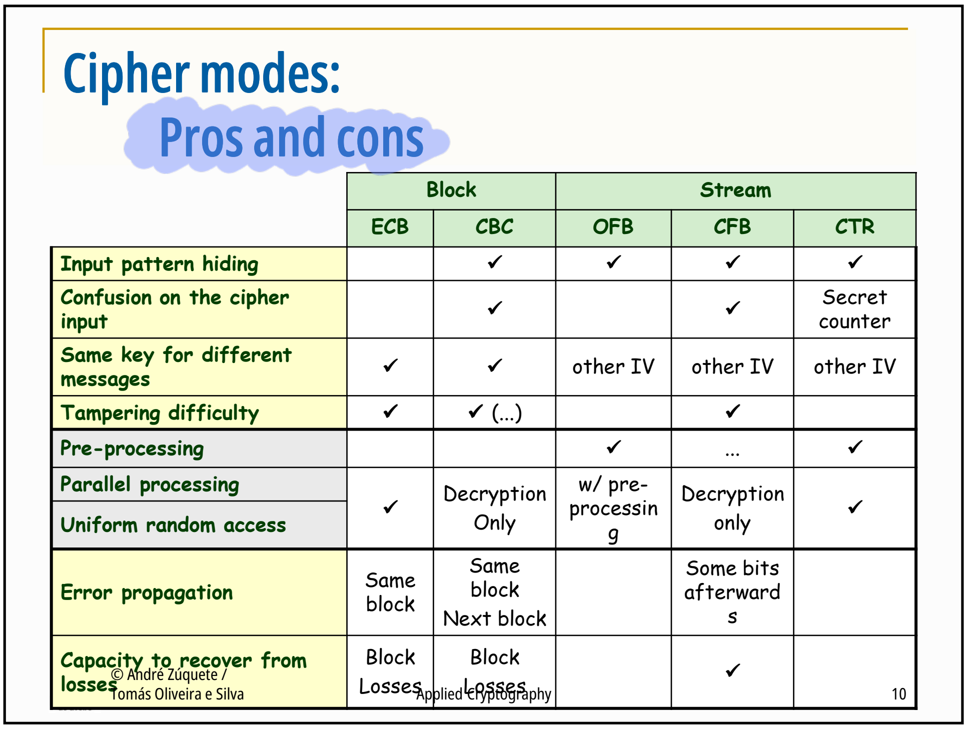
$S_i = S_{i-1}+1$
$S_0 = IV$

© André Zúquete / Tomás Oliveira e Silva

Applied Cryptography

9

Has uniform random acess.
Has parallel computation



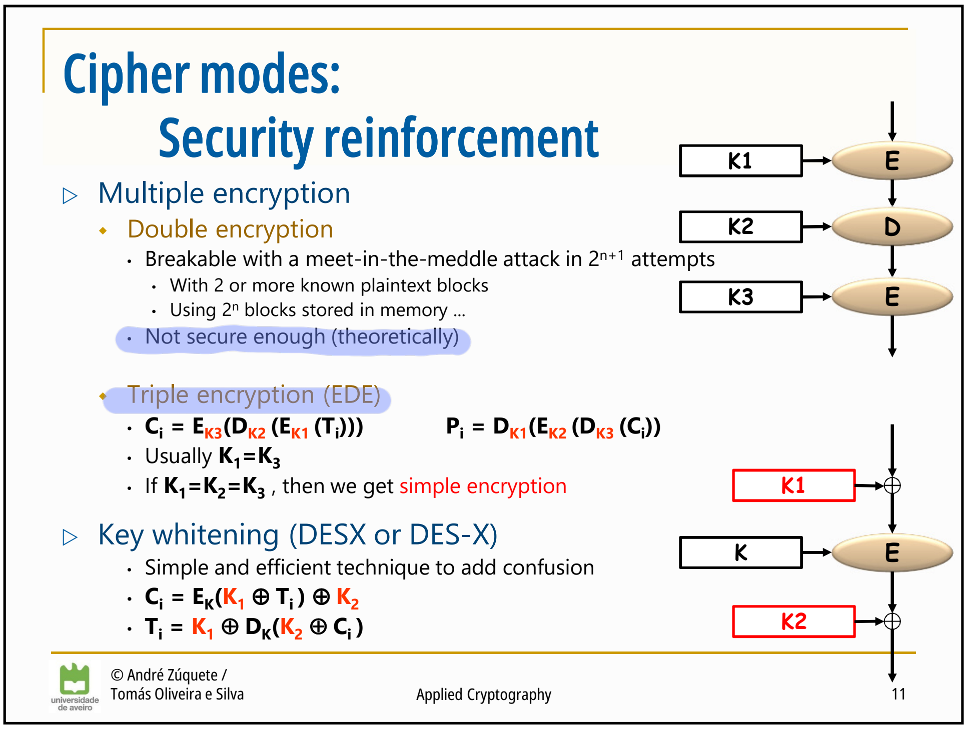
Cipher modes: Pros and cons

	Block		Stream		
	ECB	CBC	OFB	CFB	CTR
Input pattern hiding		✓	✓	✓	✓
Confusion on the cipher input		✓		✓	Secret counter
Same key for different messages	✓	✓	other IV	other IV	other IV
Tampering difficulty	✓	✓ (...)		✓	
Pre-processing			✓	...	✓
Parallel processing	✓	Decryption Only	w/ pre-processing	Decryption only	✓
Uniform random access					
Error propagation	Same block	Same block Next block		Some bits afterwards	
Capacity to recover from losses	Block Losses	Block Losses		✓	

© André Zúquete / Tomás Oliveira e Silva

Applied Cryptography

10



Cipher modes: Security reinforcement

- ▷ Multiple encryption
  - Double encryption
    - Breakable with a meet-in-the-meddle attack in 2^{n+1} attempts
      - With 2 or more known plaintext blocks
      - Using 2^n blocks stored in memory …
    - Not secure enough (theoretically)
  - Triple encryption (EDE)
    - $C_i = E_{K3}(D_{K2}(E_{K1}(T_i)))$ $P_i = D_{K1}(E_{K2}(D_{K3}(C_i)))$
    - Usually $K_1=K_3$
    - If $K_1=K_2=K_3$, then we get simple encryption
- ▷ Key whitening (DESX or DES-X)
  - Simple and efficient technique to add confusion
  - $C_i = E_K(K_1 \oplus T_i) \oplus K_2$
  - $T_i = K_1 \oplus D_K(K_2 \oplus C_i)$

© André Zúquete / Tomás Oliveira e Silva

Applied Cryptography

11

→ DEFS uses this