Tópicos Avançados em Computação I
Criptografia

- Cifras modernas

Dúvidas? *(aula anterior)*

Exercícios Anteriores

- Exemplo

Dúvidas? *(exercício - aula anterior)*

Substituição *vs.* Transposição

- O estudo de algumas técnicas de cifragem/encriptação clássicas nos permite ilustrar os conceitos básicos da criptografia simétrica utilizados até hoje.
- Este estudo permite, também, antecipar e prever técnicas de criptoanálise que possam ser empregadas para atacar uma cifra.
- Os dois blocos de montagem básicos de todas as técnicas de encriptação são: substituição e transposição.

Substituição

- A técnica de substituição é aquela em que as letras do texto claro são substituídas por outras letras, números ou símbolos; transformando-as em um texto cifrado (mensagem embaralhada).
  - Exemplo: Cifra de César

Transposição

- Por outro lado, se o texto cifrado for obtido realizando-se algum tipo de permutação das letras do texto claro, têm-se uma cifra que utiliza a técnica de transposição.
  - Exemplo:

```
Chave: 3
d a n i e l a
d     i     a
  a     e
    n     l
D I A A E N L
```

Confusão *vs.* Difusão

- Uma cifra deve obscurecer completamente as propriedades estatísticas da mensagem.
- Diz-se que uma substituição acrescenta “confusão” à informação.
- Diz-se que uma “transposição” acrescenta “difusão” à informação.

Confusão

- Confusão significa que cada dígito binário (bit) do texto cifrado deve depender de várias partes da chave, obscurecendo as conexões entre os dois.
- A propriedade de confusão oculta a relação entre o texto cifrado e a chave.
- Esta propriedade torna difícil encontrar a chave do texto cifrado e se um único bit em uma chave for alterado, o cálculo dos valores da maioria ou de todos os bits no texto cifrado será afetado.
- A confusão aumenta a ambigüidade do texto cifrado.

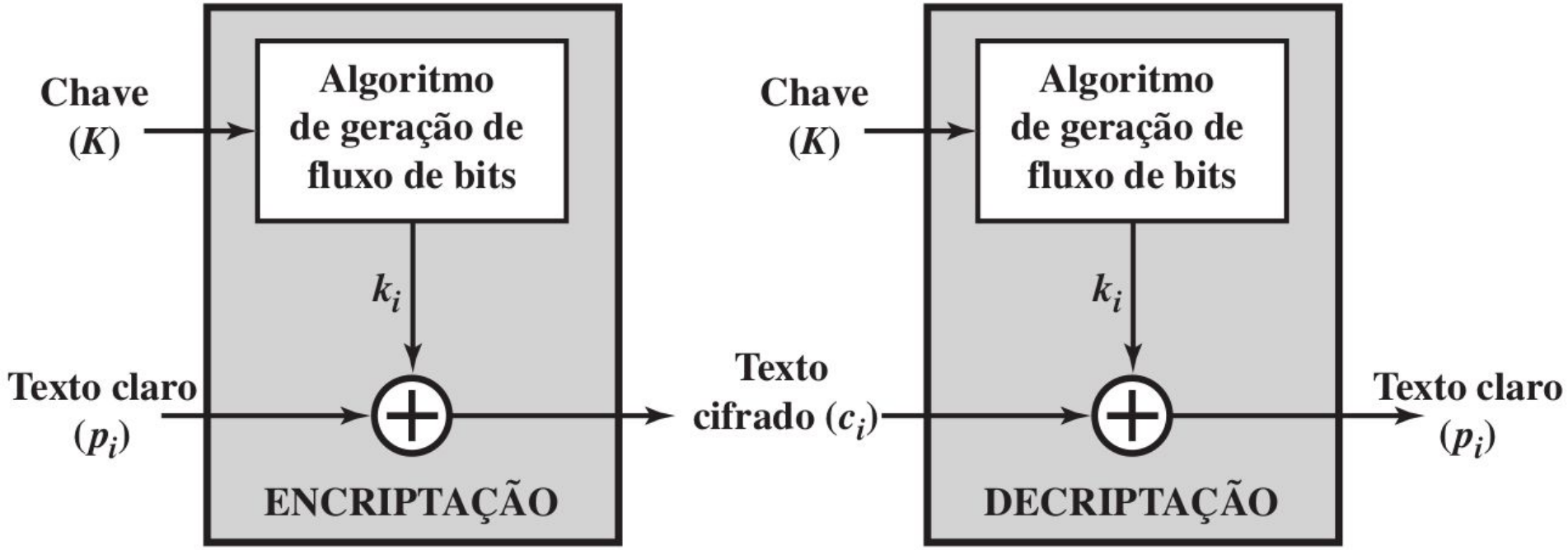
Difusão

- Difusão significa que se mudarmos um único bit do texto simples, então (estatisticamente) metade dos bits no texto cifrado deve mudar e, da mesma forma, se mudarmos um bit do texto cifrado, então aproximadamente metade dos bits do texto simples deve mudar.
- Como um bit pode ter apenas dois estados, quando todos eles são reavaliados e alterados de uma posição aparentemente aleatória para outra, metade dos bits terá o estado alterado.
- A ideia de difusão é esconder a relação entre o texto cifrado e o texto as claras.

Exemplo de cifra

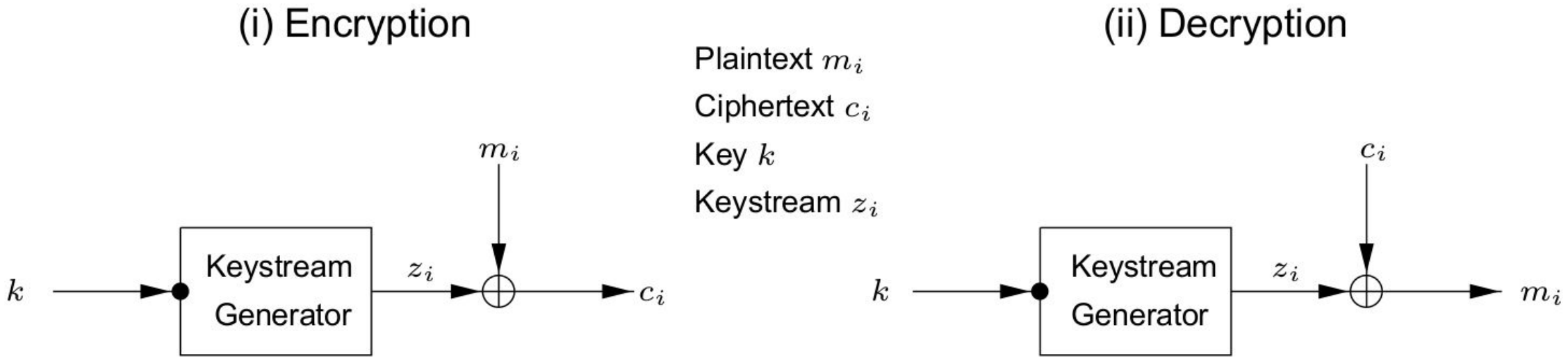
- Desenvolver colaborativamente!

Cifra de fluxo *(Stream Cipher)*

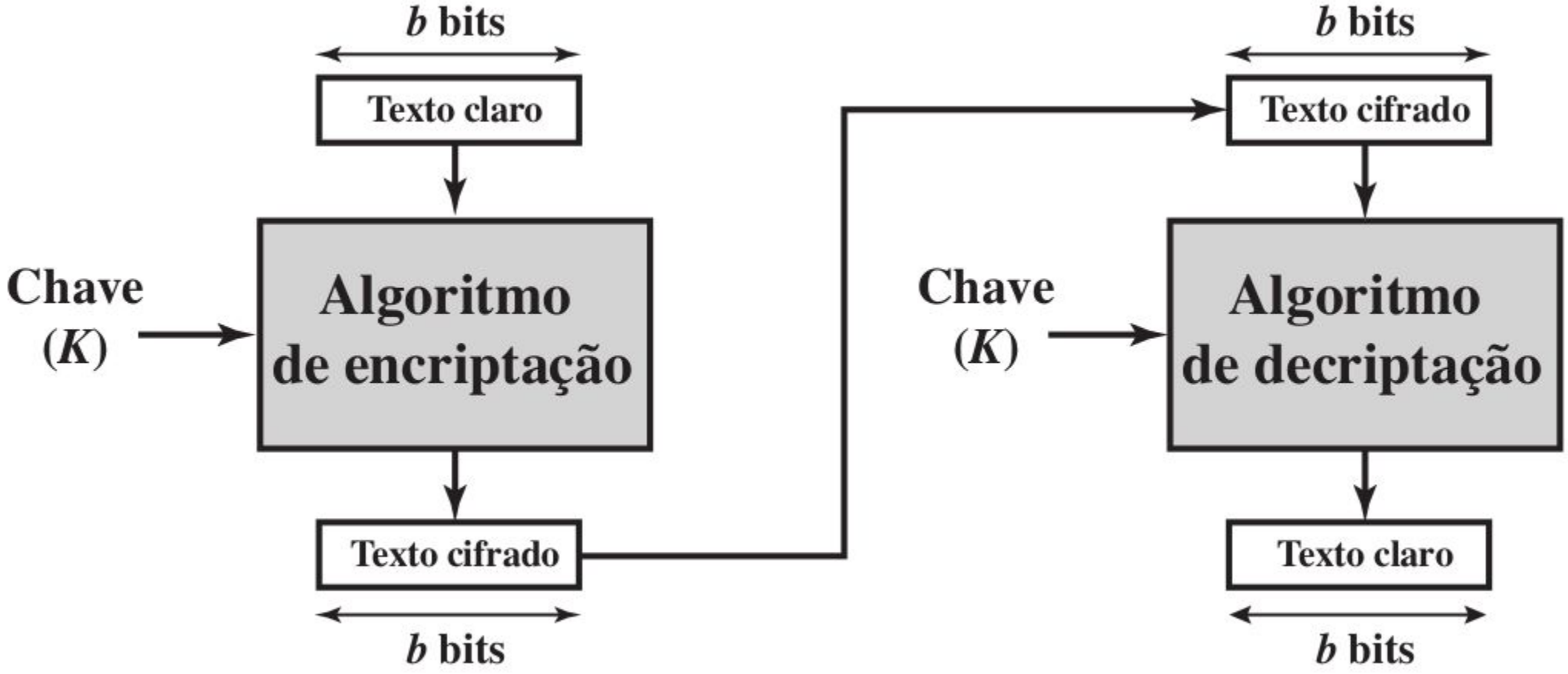


(a) Cifra de fluxo usando gerador algorítmico de fluxo de bits

Cifra de fluxo *(Stream Cipher)*

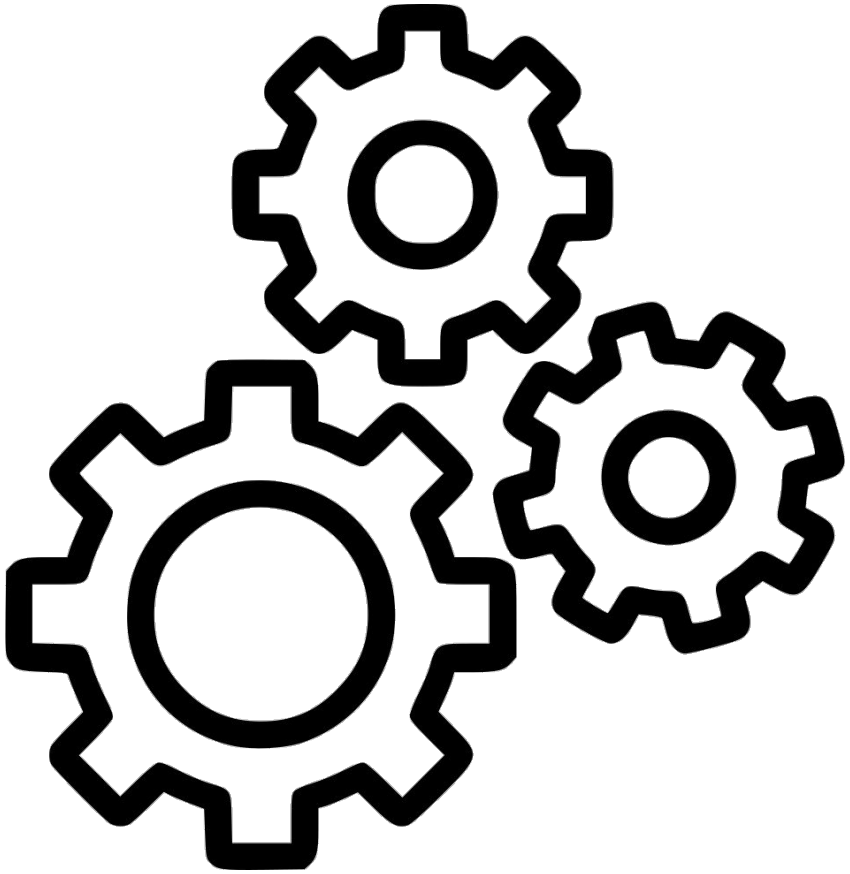


Cifra de bloco *(Block Cipher)*

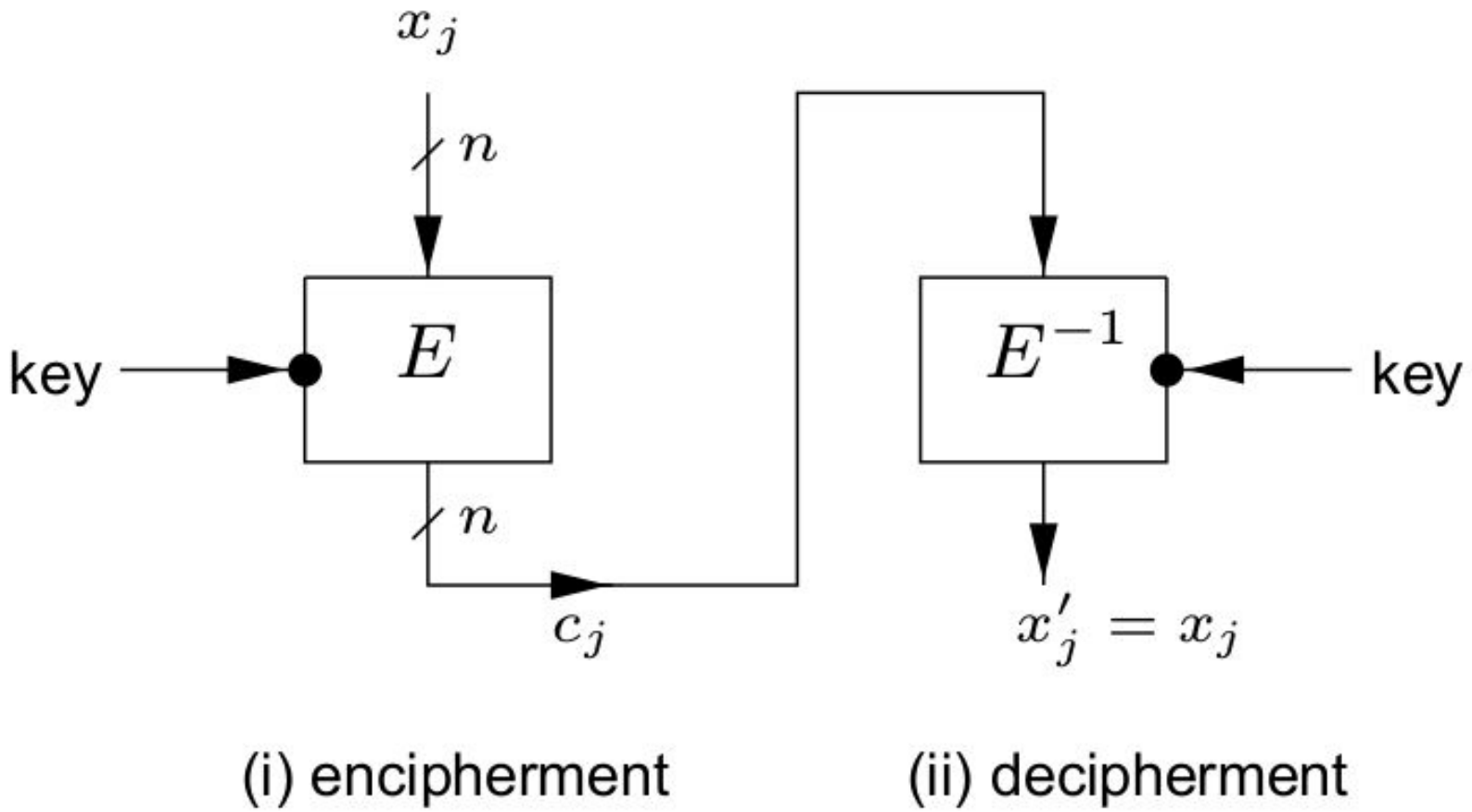


(b) Cifra de bloco

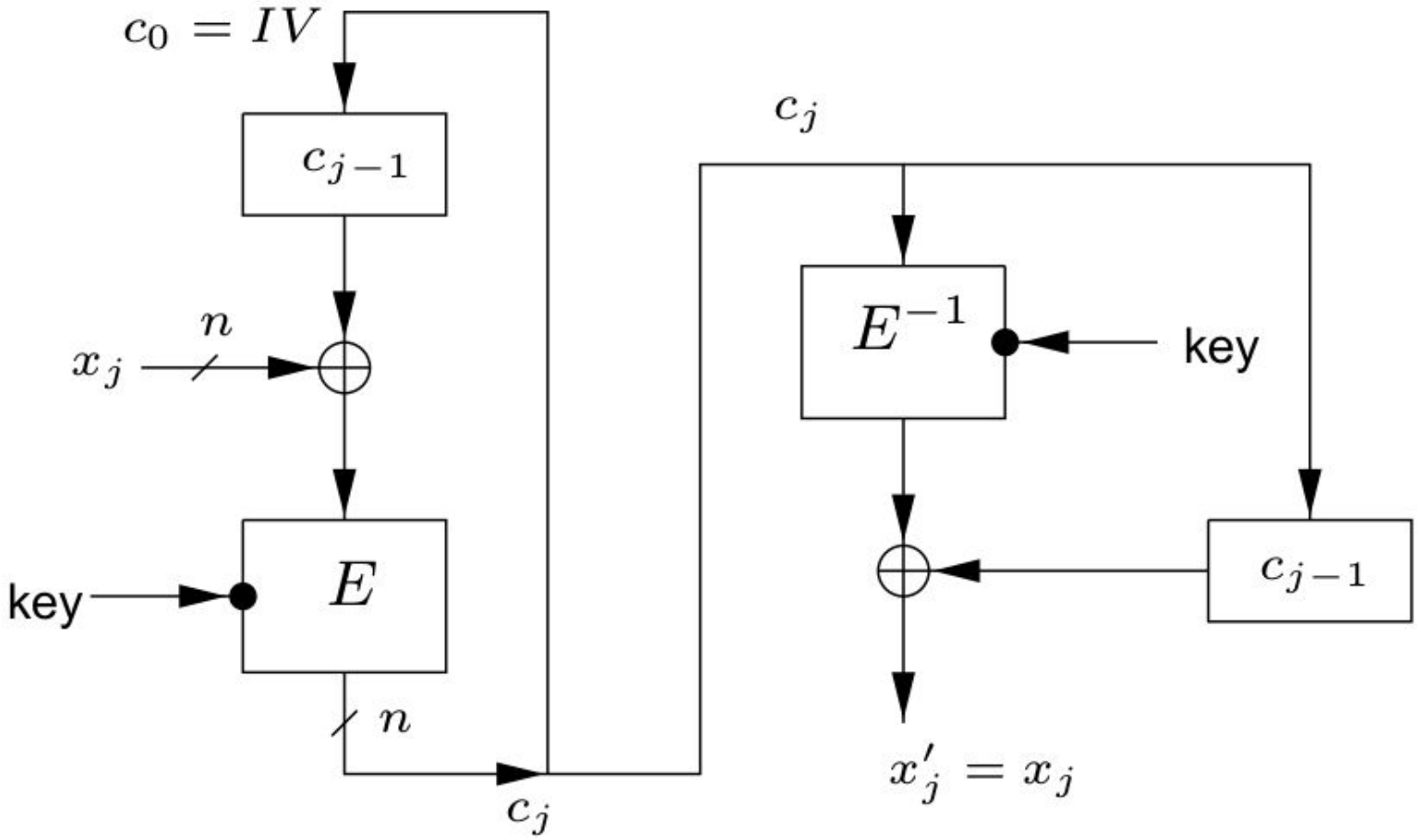
Cifra de bloco *(Block Cipher)* - Modos



Electronic Codebook (ECB)

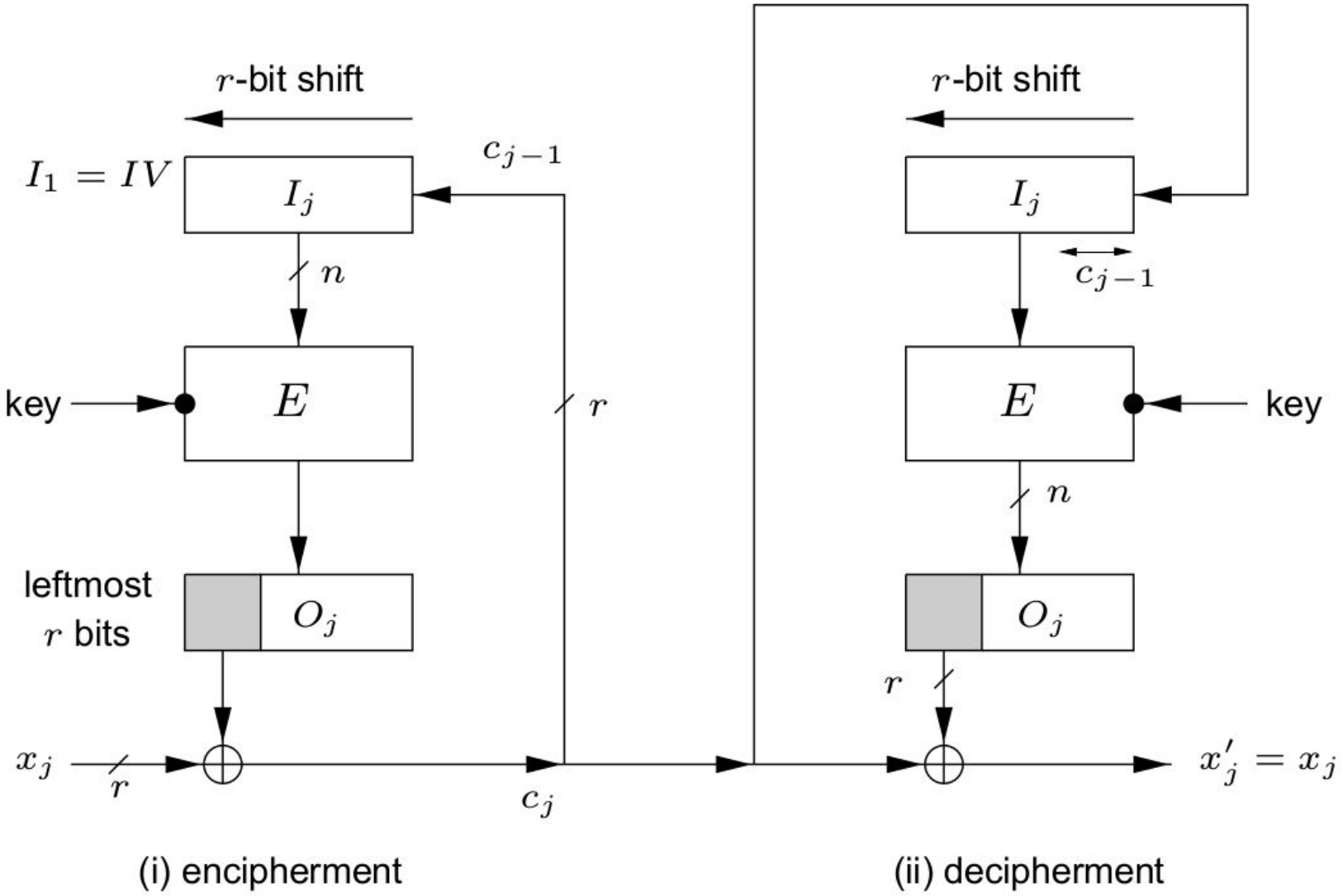


Cipher-block Chaining (CBC)

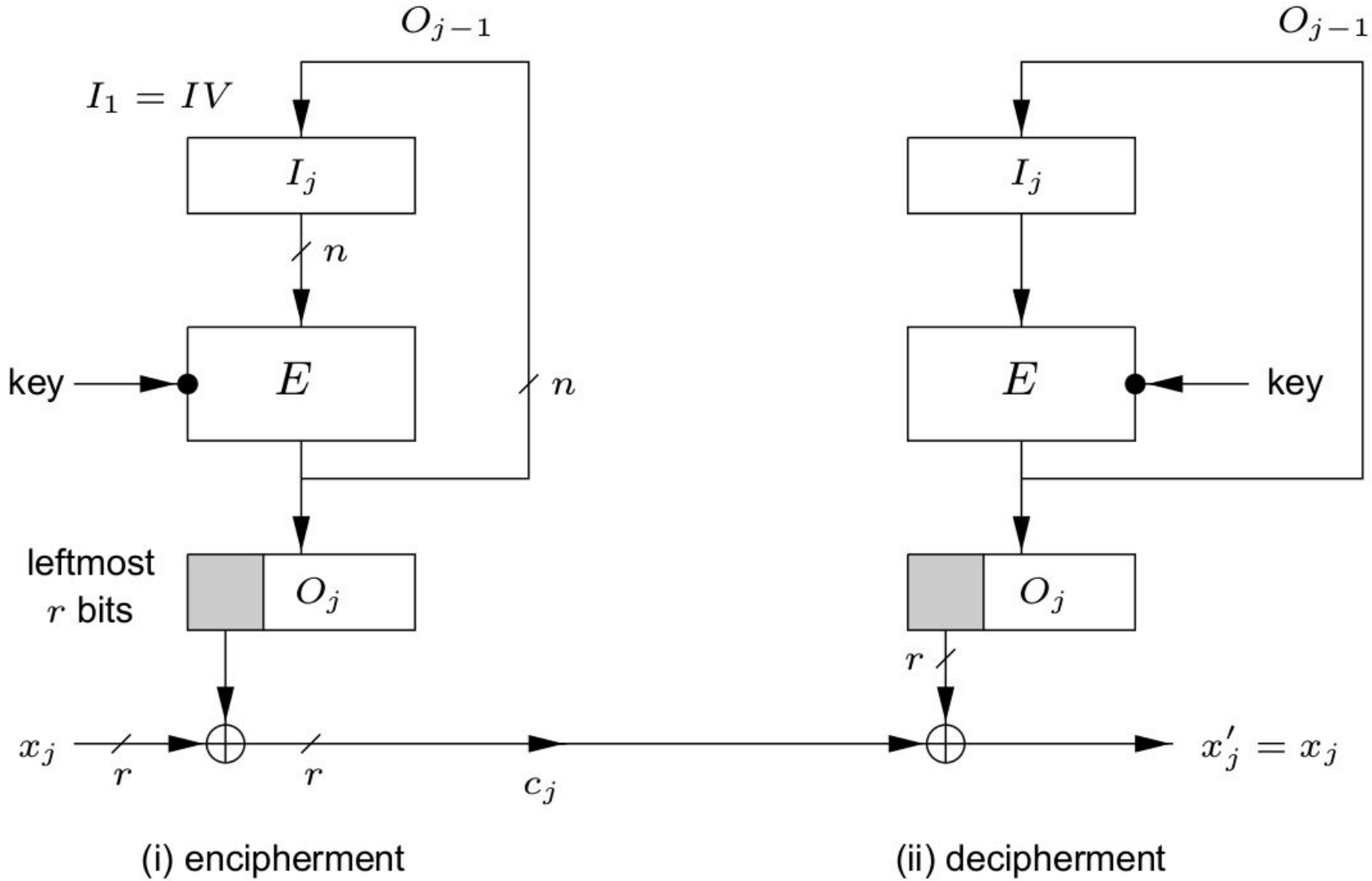


(i) encipherment (ii) decipherment

Cipher feedback (CFB)



Output feedback (OFB)



Exercício de Programação 01

Crie um software que possa encriptar e decriptar usando qualquer modelo de cifra simétrica.

Obrigado!

ewerton.andrade@unir.br
http://ewerton.andrade.pro.br/