Block Ciphers

Teórica #3 de Criptografia Aplicada

Block Ciphers (Cifras de bloco)

O que são cifras de bloco?

Uma cifra de bloco é definida por dois algoritmos deterministicos, que tem uma funcionalidade extremamente **limitada** (só funcionam para blocos de tamanho B, ou seja dado um input com tamanho B o bloco terá o tamanho B).

Cifras de bloco são inverteis e por sua vez injetivas, e como tem o mesmo tamanho no input e output são permutações (invertivel = que se pode reverter = decriptar).

Chave define uma permutação, e dado o seu tamanho lambda, no máximo temos 2^lambda permutações.

Segurança em Cifras de Bloco

Cada cifra de bloco deve ser uma permutação **pseudorandom** (PRP).

Um atacante tenta descobrir o texto original e então faz uma vasta procura das encriptações:

NAO PERCEBI MUITO BEM O QUE É UMA PERMUTAÇÃO PSEUDOALEATORIA

Diferenças entre permutações pseudoaleatórias e permutações aleatórias:

- Não existem repetições de permutações;
- Blocos de cifra parecem totalmente aleatórios;
- Inputs diferentes levam a outputs independentes;
- Deve ser impossível recuperar a chave, caso contrario é possível descobrir o texto a ser cifrado que leva à permutação.

Tweakable Block Ciphers

Variante das cifras de bloco onde é acrescentada mais uma "camada" de segurança, ao acrescentar um valor de ajuste (tweak) no input da encriptação e decriptação.

Block Size

Antigamente: tamanhos de bloco de 64 bits (DES - Data Encryption Standard)

Mais recentemente: tamanhos de bloco de 128 bits (AES - Advanced Encryption Standard)

O tamanho dos blocos deve ser moderado: não pode ser muito pequeno porque o tamanho dos blocos também serve como parâmetro de segurança da cifra, mas também não podem ser muito grandes se não as implementações em Hardware/Software tornam-se ineficientes.

Como são as cifras de bloco construídas?

Cifras iterativas: rondas

Cifra de bloco itera um algoritmo de ronda *n* vezes, sendo que cada ronda toma uma chave diferente:

- **Chave de ronda** derivada de uma chave da cifra de bloco;
- Sequencia de **chaves de ronda** de nome *key schedule*.

Exemplo de encriptação: **E**(*K*, *P*) := R(...R(R(P, K1), K2,)...Kn)

Existem **dois** padrões para construção de cifras de bloco:

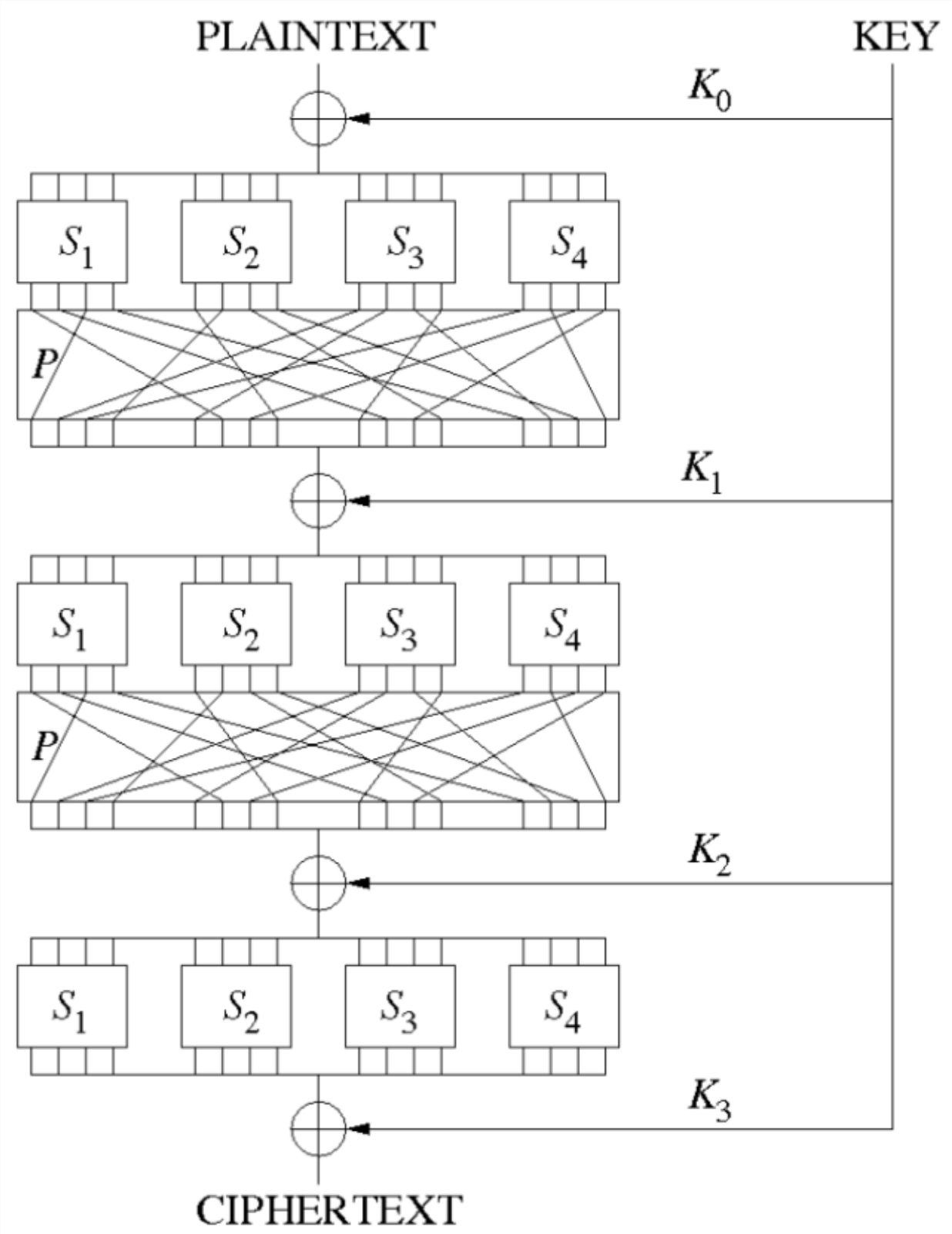
- Substitution-Permutation Network (SPN);
- ...

Substitution-Permutation Network

Nestas redes, a função de ronda é uma camada de Substitution-Permutation:

- **Substitution** é representada por *S-boxes*, tabelas de consulta pequenas (4-8 bits), desenhadas para introduzir (não linearidade) na função de ronda. Estas por si criam a propriedade de *confusão* no bloco;
- **Permutation** é representado por transformações bit-level (e.g., switches) ou por funções algébricas que introduzem dependências ao longo de todo o bloco (propriedade de *difusão*).

Exemplo de uma cifra de bloco que é construída sobre este padrão: **AES**.



Feistel Network

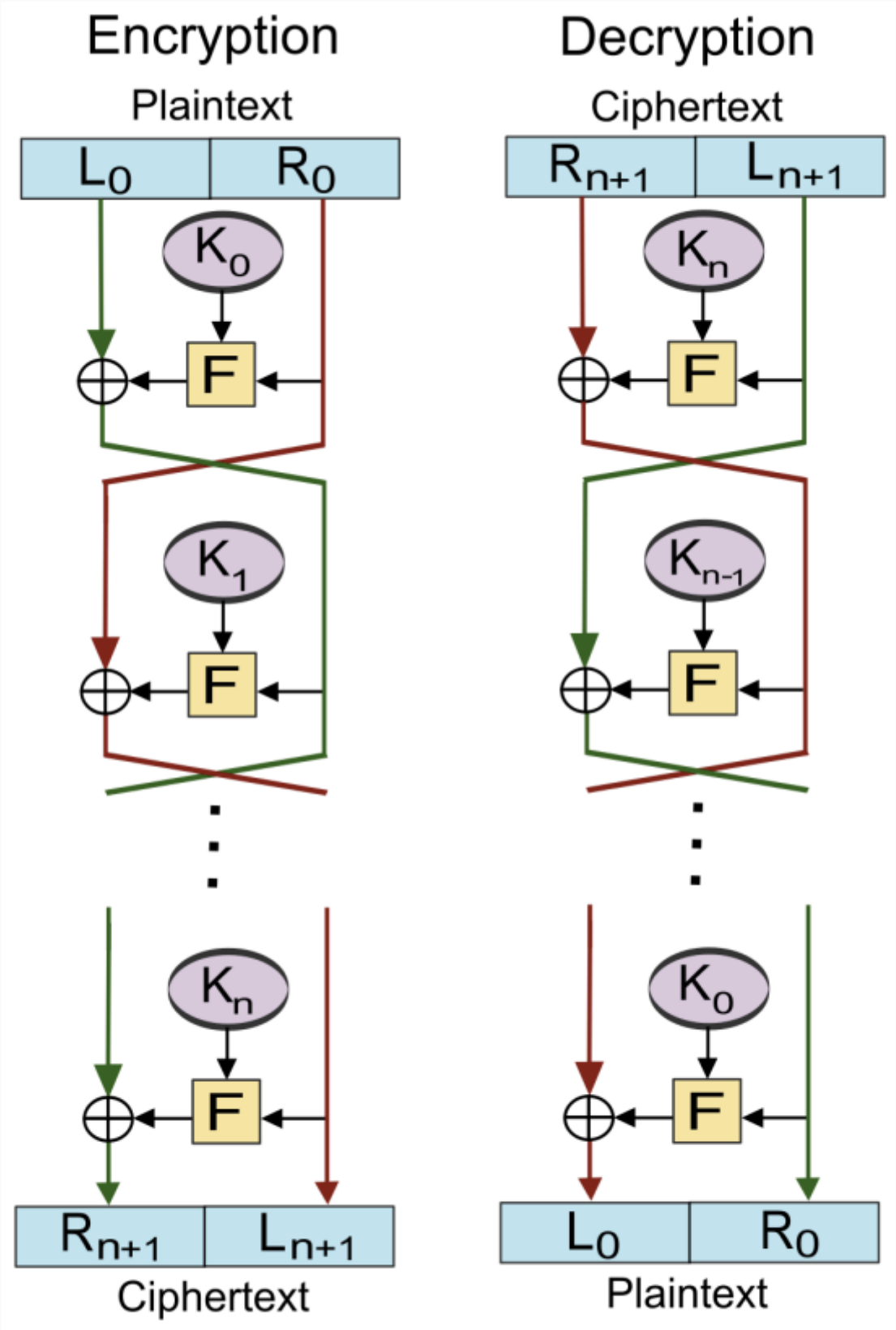
Teve bastante importância no nível do hardware, pois tem como objetivo garantir que o circuito de hardware utilizador para fazer a cifra é o mesmo para a decifrar, mudando apenas os inputs (plain text - encriptar e texto encriptado - decriptar).

Funciona da seguinte maneira: dado um block de input, é divido a meio de forma a gerar o par (L, R). Ao R, é aplicado a função de ronda e utiliza-se o L para mascar o mesmo. Na iteração seguinte, utiliza-se o output da mascara como R, ou seja utiliza-se a função de ronda no output da mascara e o R original como input para a mascara.

```
Bloco a encriptar -> (L, R)
R' = Fronda (R)
M = L XOR R'
M' = Fronda (M)
M'' = R XOR M'
….
```

Para decriptar, inverte-se a ordem das chaves.

Exemplo de uma cifra de bloco que é construída sobre este padrão: **DES** e **GOST**.



A função de ronda pode ser uma PRP ou PRF e o tamanho do input pode ser diferente do output.

3DES

3DES = Aplicação do DES três vezes com chaves independentes (diferentes).

AES

Criado por motivação ao provar-se que DES não era seguro. Foi criado através de um concurso de criptografia que demorou 3 anos, lançado pela NIST. Foi utilizado como modo defesa a heurística, sendo este aberto a propostas e atacado pelo resto da comunidade (participantes). Foi criado com o objetivo de ser eficiente (performance) e resistente a cryptanalysis.

Tamanho do bloco: 128-bit

Chaves de 128, 192 e 256 bits.

Mantém um estado interno de 128-bits, sendo os estados pertencentes a uma matriz de 4x4 (16 estados).

É implementado segundo o padrão SPN.

Não existe prova matemática que o AES é uma PRP.

Symmetric Encryption with Block Ciphers

Modos de Operação

Historicamente, cifras de bloco eram usadas em diferentes modos de operação para encriptar informação.

Nos dias de hoje, a criptografia tenta esclarecer várias coisas:

- Cifras de bloco são primitivas (algo atómico que nos permite construir outras coisas - building block);
- Por si, cifras de bloco por si são “useless”;
- Existem muitas maneiras de encriptar de forma insegura com uma cifra de bloco;
- O que se pretende é construir esquemas de encriptação através de cifras de bloco, pois estes tem as suas próprias definições de segurança.

Cifra Simétrica

Tipicamente encriptação é um algoritmo probabilístico, enquanto que o de decriptação, determinístico.

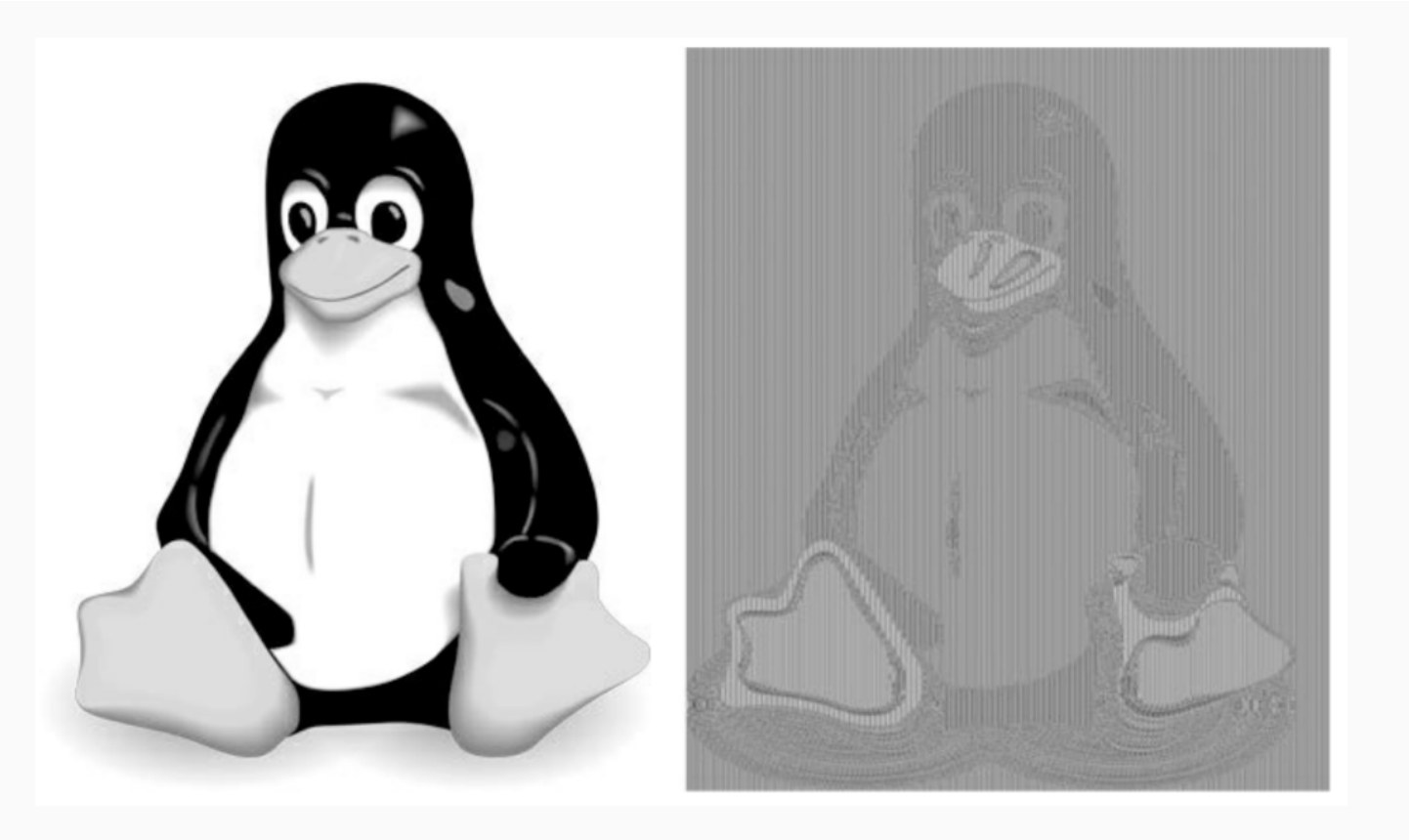
A mensagem a encriptar pode ter *qualquer tamanho (nao tem que satisfazer as condições do tamanho do bloco)*.

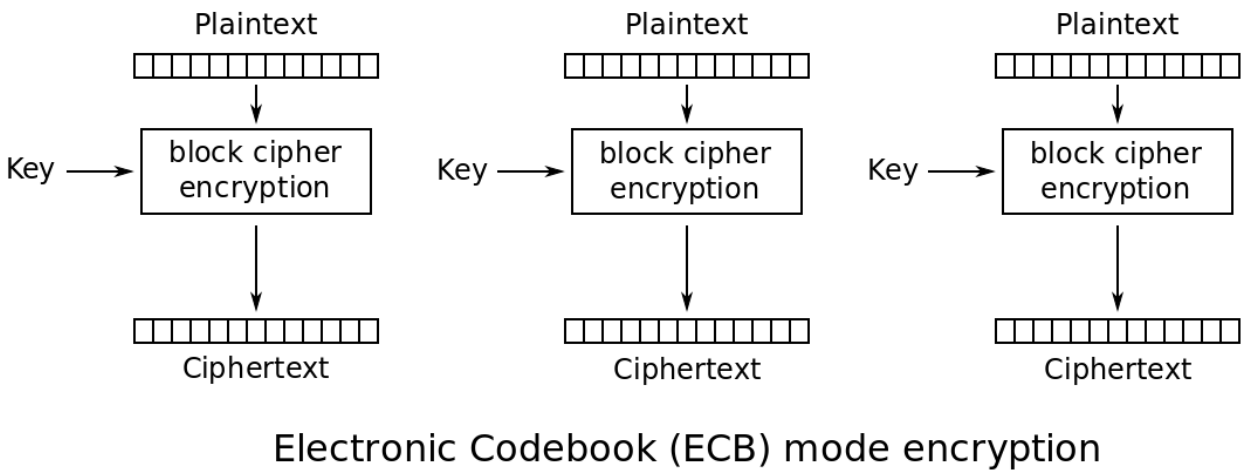
NAO PERCEBI MUITO BEM O IND-CPA

ECB - Electronic-Code-Book Operation Mode

Modo mais simples de cifra simétrica e por sua vez o mais inseguro de todos.

A mensagem é dividida em múltiplos blocos, sendo que o ultimo bloco pode precisar de padding, de forma a que o tamanho do bloco da cifra se mantenha. Inseguro no sentido que para blocos de cifra iguais, o output é o mesmo.





Electronic Codebook (ECB) mode encryption

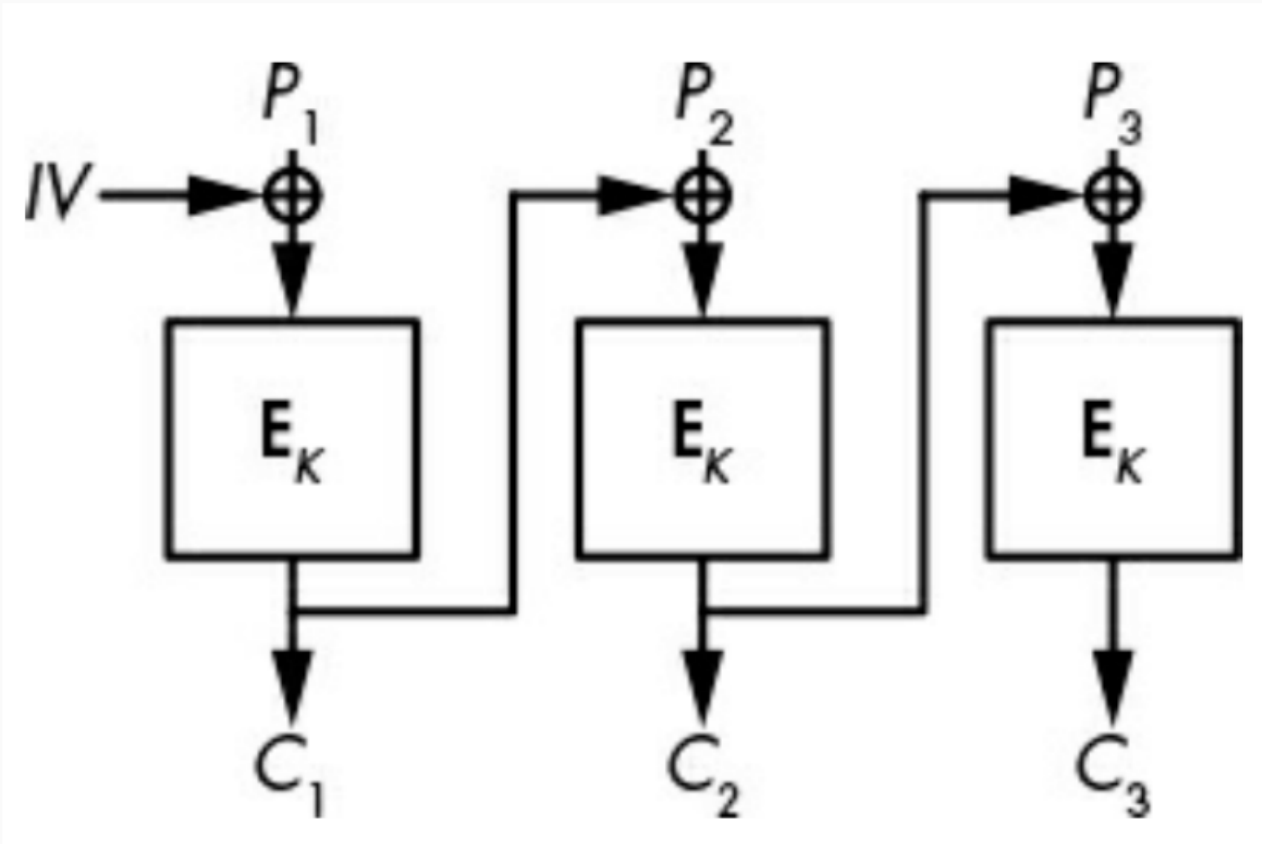
Problema ECB => Inputs Iguais = Outputs iguais => Falta de difusão

CBC - Cipher Block Chaining Operation Mode

Requer um IV - Initialization Vector (estilo de uma chave pseudoaleatória ou única), que é aplicado no XOR da primeira mascara do primeiro bloco a cifrar. Nos seguintes blocos, é utilizado o output

do bloco cifrado como IV da mascara.

```
Plain text -> B{B1, B2, B3, …, Bn}
M1 = B1 XOR IV
C1 = E(M1, K)
M2 = B2 XOR C1
C2 = E(M2, K)
….
```



Existe muito menos probabilidade do output ser igual ao input. Encriptação do mesmo plain text com IVs diferentes são sempre independentes (isto significa que CBC satisfaz IND-CPA, porque é um PRP.

Na fase de decifração, é revertido o processo ao aplicar o bloco de cifra na função de encriptação e de seguida utilizar a cifra de bloco anterior na função XOR, para obter a mensagem que foi cifrada, ou seja:

`Pn = E(Cn, K) XOR Cn−1`

Isto permite-nos concluir que é possível decriptar uma mensagem previamente encriptara em CBC não conhecendo o IV, pois apenas é preciso jogar com os blocos e reverter o processo (mas a chave é sempre necessária). Se mudarmos um bloco de cifra, todos os seguintes são corrompidos no sentido em que não podem ser decriptados, mas os anteriores sim.

Cifragem é **sequencial** mas a decifragem pode ser feita em **paralelo**.

Esquemas de Padding

Como cifras de bloco requerem que todos os blocos sejas de tamanho igual ou múltiplo do estabelecido, é necessária adicionar padding às mensagens a cifrar quando estas não cumprem o tamanho do bloco. Padding significa “adicionar espaço” a algo, neste caso acrescentar bytes para satisfazer os requisitos do tamanho do bloco.

CTR - Counter (Operation) Mode

Trabalha-se com o contadores (valor númerico) como vetor de inicialização.

Opera de forma semelhante ao CBC, mas em vez do input da função criptográfica ser a mensagem plain text, no CTR a mensagem é substituída por uma stream de contadores {0, 1, 2, 3, ... N}. Depois na fase da mascara, o XOR é aplicada ao bloco da mensagem plain text.

Nonce CTR Mode aplica a noção de um nonce (number used only once) truncado ao valor do contador para cada bloco a cifrar.

Não requer padding.

O CTR é bastante eficiente pois:

- permite a paralelização da encriptação e decriptação dos blocos;
- diferentes blocos podem ser atualizados, e consequentemente decriptados de novo, desde que não se perca o contador.