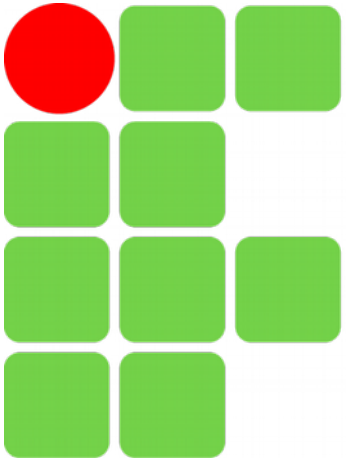


INSTITUTO FEDERAL
SANTA CATARINA

Segurança Computacional

Ciência da Computação

Robson Costa
(robson.costa@ifsc.edu.br)

Modos de Cifras

Introdução

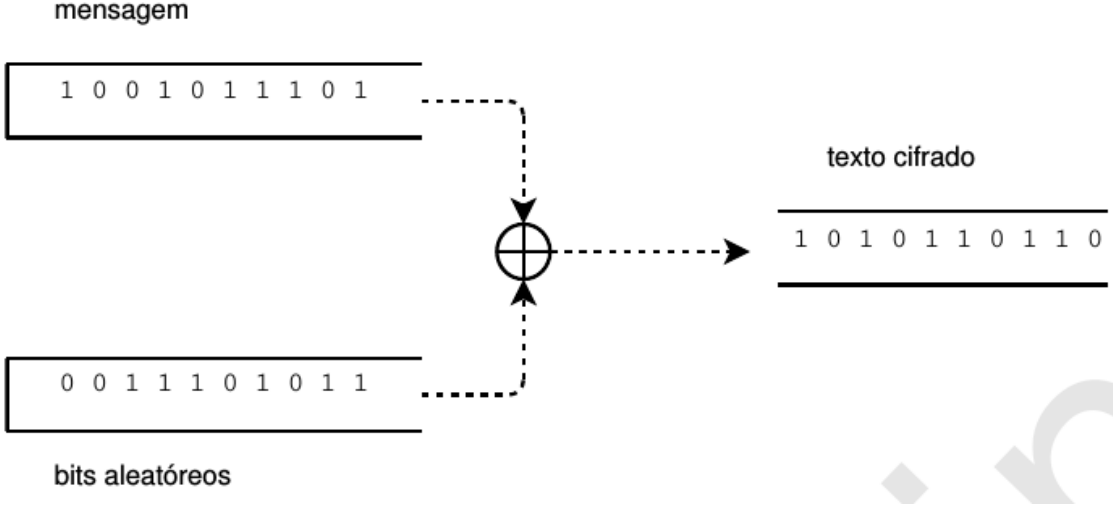
- Ao algoritmo usado para realizar as funções de criptografia e decriptografia damos o nome de **cifra**;
- Cifras podem ser classificados em dois tipos:
  - **Cifras de Fluxo**;
  - **Cifras de Blocos**;

Modos de Cifras

Cifras de Fluxo

- Transformam cada bit da mensagem em um bit do texto cifrado ao misturá-lo com um bit de outra fonte de bist (ex.: um gerador pseudoaleatório de bits);

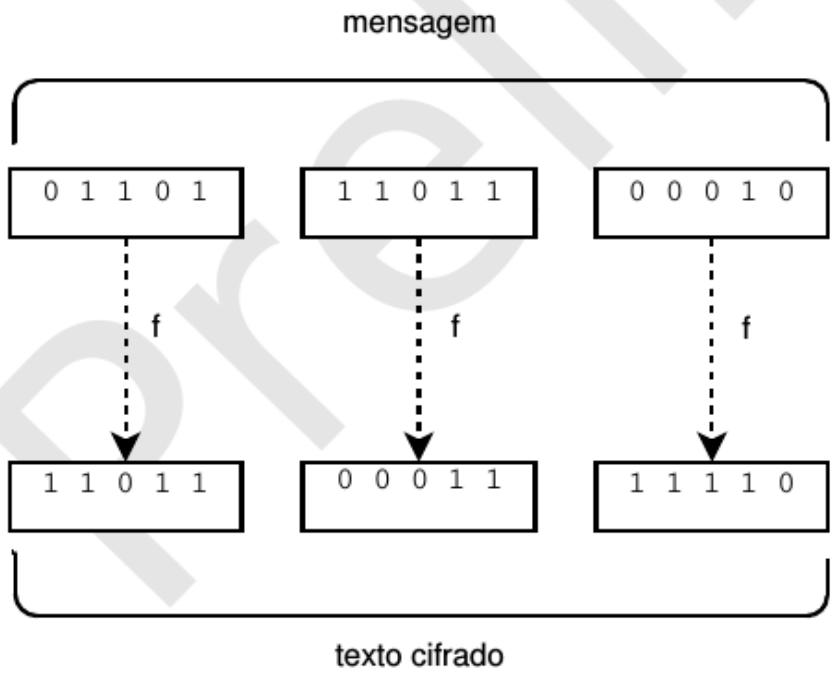
- Esta mistura comumente é realizada por uma operação **XOR** (ou exclusivo);
  - A semente do gerador aleatório é a senha que permite encriptar e decriptar as mensagens;



Modos de Cifras

Cifras de Bloco

- Transformam uma sequências de bits de tamanho fixo, realizando nelas transformações difíceis de inverter;
- A função *f(k,m)* abaixo aceita dois parâmetros: a chave secreta e a mensagem;



Modos de Cifras

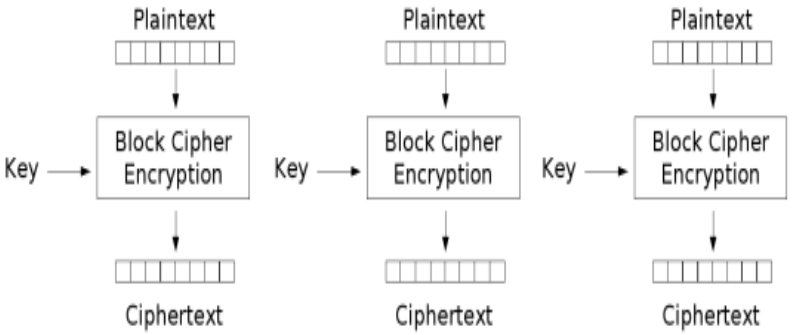
Tipos

- ECB (*Electronic Code Book*);
- CBC (*Cipher Block Chaining*);
- CFB (*Cipher FeedBack*);
- OFB (*Output FeedBack*);
- SCM (*Stream Cipher Mode*);
- CTR (*Counter Mode*);

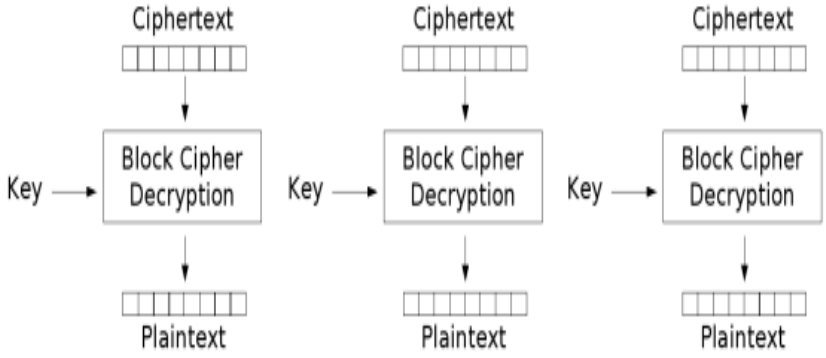
Modos de Cifras

ECB (*Electronic Code Book*)

- O modo mais simples para se obter cifras;
- É adequado à cifras de pequenas quantidades de dados aleatórios, como números de cartões de crédito;
- A técnica consiste em dividir a mensagem em blocos de tamanho adequado, cifrar os blocos separadamente e concatenar os blocos cifrados na sua respectiva ordem;



Electronic Codebook (ECB) mode encryption



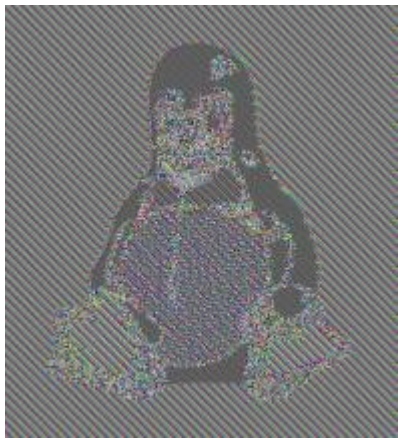
Electronic Codebook (ECB) mode decryption

Modos de Cifras

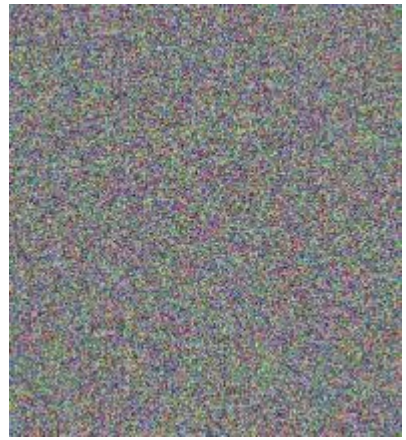
ECB (*Electronic Code Book*)

- A desvantagem desta técnica é que blocos contendo mensagens originais idênticas irão produzir blocos cifrados idênticos;
  - Esta não é uma característica desejável, uma vez que desta forma não se pode ocultar padrões de dados;

Imagem original.



Criptografada utilizando modo ECB.



Criptografada utilizando outro modo.

Modos de Cifras

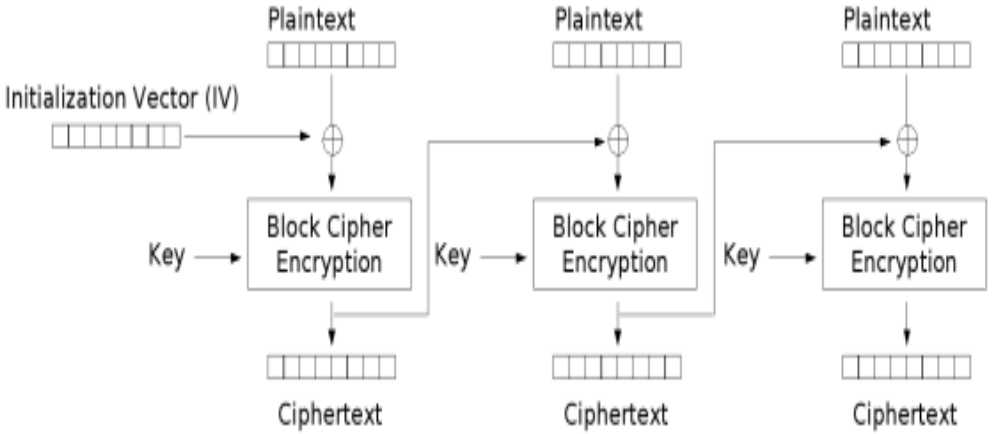
CBC (*Cipher Block Chaining*)

- Cada bloco de texto claro é **submetido a uma operação XOR com o bloco de texto cifrado anterior**, antes de ser criptografado por algum algoritmo de criptografia;
  - Em uma operação lógica **XOR** entre dois operandos o valor é verdadeiro se e somente se um dos operandos possuir um valor verdadeiro;
- Consequentemente, o mesmo bloco de texto claro não é mais mapeado para o mesmo bloco de texto cifrado (fraqueza do ECB);
- Assim, a criptografia não é mais uma grande cifra de substituição monoalfabética;
- O primeiro bloco de texto claro é submetido a uma **operação XOR** com um **vetor de inicialização** (IV), escolhido ao acaso, o qual tem que ser transmitido (em texto claro) juntamente com o texto cifrado;

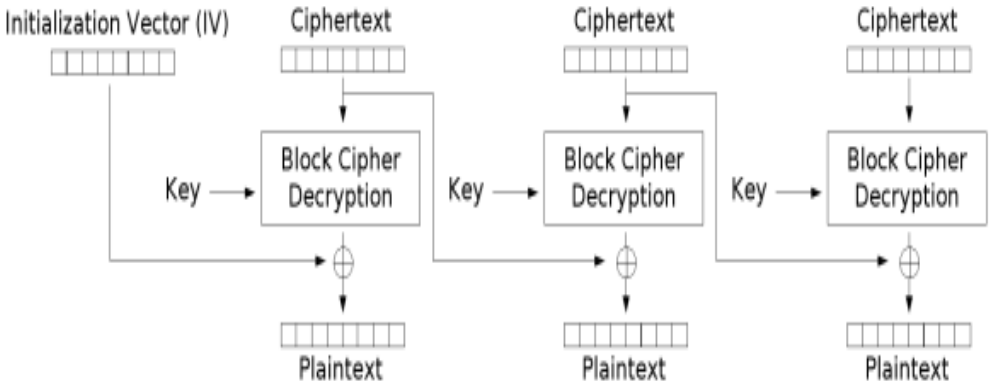
Modos de Cifras

CBC (*Cipher Block Chaining*)

- O vetor de inicialização (IV) objetiva aumentar a segurança da cifra introduzindo um grau de aleatoriedade;
- Este vetor de ser único, mas igual tanto na cifragem quanto na decifragem;



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Modos de Cifras

CBC (*Cipher Block Chaining*)

- O CBC utiliza um encadeamento de blocos e cifras;

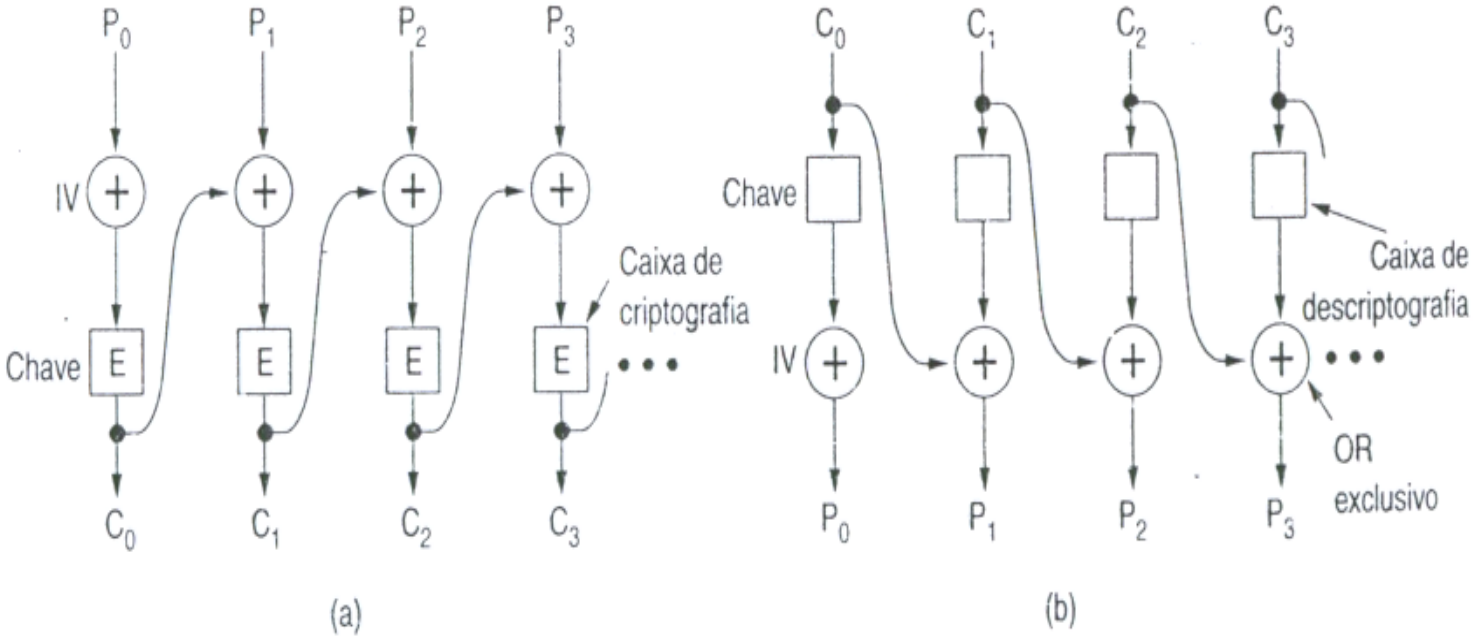


Figura 8.12 Encadeamento e blocos de cifras. (a) Codificação. (b) Decodificação

Modos de Cifras

CBC (*Cipher Block Chaining*)

- Diferentemente do CBC, no ECB a criptografia de um bloco *i* é uma função somente do texto claro *i*;
- No CBC, a criptografia de um bloco *i* é uma função de todo o texto claro contido nos blocos *0* a *i-1*;
- Assim, o mesmo texto claro gera um texto cifrado diferente, dependendo de onde ele ocorre;
- A **vantagem** do encadeamento de blocos de cifras é que o mesmo bloco de texto claro não resultará no mesmo bloco de texto cifrado;
- A **desvantagem** do encadeamento de blocos de cifras é que o processo é sequencial, não podendo ser paralelizado;

Modos de Cifras

CBC (*Cipher Block Chaining*)

- Outra característica é que a mensagem deve ser alinhada de acordo com um múltiplo do tamanho do bloco de cifra (64 bits ou 128 bits);

- A criptoanálise se torna difícil;
  - Acaba por ser a principal razão do seu uso;

- Útil quando se pretende cifrar grandes quantidades de dados, como arquivos, apresentando uma segurança significativamente superior ao modo ECB;

Modos de Cifras

CFB (*Cipher FeedBack*)

- Mais adequado para cifrar quantidades pequenas de dados (bytes ou blocos pequenos), como por exemplo bytes individuais que formam um stream (de bytes);
- Assim como no CBC, no CFB é necessário utilizar um vetor de inicialização (IV) para iniciar o processo;
- O IV funcionará como um **registrador de deslocamento R** (*shift register*), formado por bytes, e que pode ter um comprimento de 64 bits (DES) ou 128 bits (AES);

Modos de Cifras

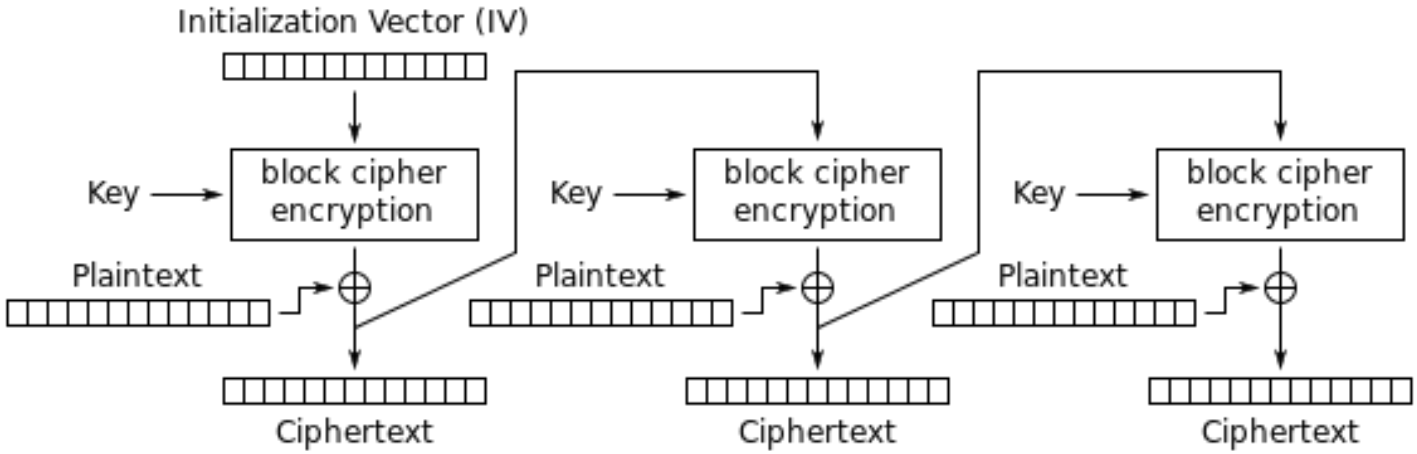
CFB (*Cipher FeedBack*)

- A cifragem com o CFB se inicia com a inicialização aleatória do IV em R;
- O algoritmo de criptografia (DES, AES) opera sobre o registrador de deslocamento para gerar um texto cifrado do tamanho do registrador (64 ou 128 bits);
- O byte da extremidade mais à esquerda do registrador de deslocamento R é selecionado;
- Uma operação XOR é feita com o byte da vez, do texto claro *P*;
- Esse byte é cifrado e transmitido;
- O registrador é deslocado 8 bits à esquerda, fazendo com que o seu byte mais à esquerda fique fora da extremidade mais à esquerda e o byte C (cifrado depois de XOR) seja inserido na posição que ficou vaga na extremidade do registrador mais à direita;

Modos de Cifras

CFB (*Cipher FeedBack*)

- O conteúdo do registrador de deslocamento R depende do histórico anterior dos bytes do texto claro P;
- Assim, o padrão que se repetir várias vezes no texto claro será criptografado de maneira diferente do texto cifrado a cada iteração;

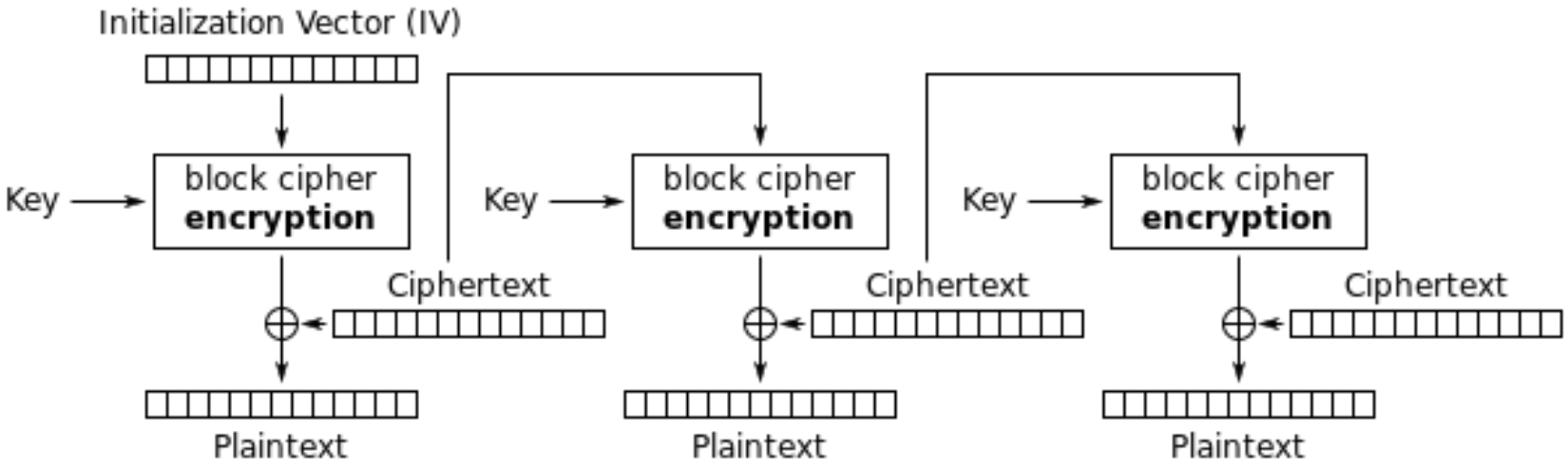


Cipher Feedback (CFB) mode encryption

Modos de Cifras

CFB (*Cipher FeedBack*)

- Na decifragem, as operações são similares as de cifragem;
- Em particular, o conteúdo do registrador de deslocamento R (é cifrado e não decifrado), ou seja, recebe o byte que vem cifrado na transmissão;



Cipher Feedback (CFB) mode decryption

Modos de Cifras

CFB (*Cipher FeedBack*)

- Desde que os dois registradores de deslocamento R (no transmissor e no receptor) permaneçam idênticos, a decifragem funcionará corretamete;
- Se um bit do texto cifrado for invertido acidentalmente durante a transmissão, os bytes no registrador de deslocamento R no receptor, serão danificados, enquanto o byte defeituoso estiver no registrador de deslocamento;
- Depois que o byte defeituoso for empurrado para fora do registrador de deslocamento, o texto claro volta a ser gerado normalmente;
- Desta forma, os efeitos de um bit invertido são relativamente fáceis de serem localizados e não destroem a mensagem como um todo;
- Porém, destroem uma quantidade de bits igual ao comprimento do registrador de deslocamento R;

Modos de Cifras

OFB (*Output FeedBack*)

- O módo OFB é análago ao CFB, mas é utilizado em aplicações em que a propagação de erros não pode ser tolerada;

Modos de Cifras

SFM (*Stream Cipher Mode*)

- Em aplicações onde um erro de transmissão de 1 bit (inversão de bit) altera 64 bits de texto claro e isto pode resultar em um impacto muito grande;
- Nesta caso são utilizadas cifras de fluxo;
- Funciona, inicialmente, criptografando um vetor de inicialização (IV) com uma chave secreta para se obter um bloco cifrado de saída;
- Este bloco de saída cifrado é então criptografado, usando-se a chave secreta para se obter um segundo bloco cifrado de saída;
- Este segundo bloco é criptografado com a chave secreta para se obter um terceiro bloco de saída cifrado, e assim por diante...

Modos de Cifras

SFM (*Stream Cipher Mode*)

- Desta forma, é criada um sequência de blocos cifrados de saída, arbitrariamente grande, de blocos cifrados de saída concatenados;
- Essa sequência é chamada de **fluxo de chaves**;
- A sequência formando o **fluxo de chaves** é tratada como uma **chave única** e submetida a uma **operação XOR** com o texto claro;
- Observe que o **fluxo de chaves** formado é **independente dos dados** (texto claro), e portanto, pode ser calculado com antecedência, se necessário;
- A decifragem ocorre gerando-se o mesmo fluxo de chaves no receptor;
- Como o fluxo de chaves só depende do IV e das chaves geradas, ele não é afetado por erros de transmissão no texto cifrado;

Modos de Cifras

SFM (*Stream Cipher Mode*)

- Desse modo, um erro de transmissão em 1 bit no texto cifrado resulta em um erro de apenas 1 bit no texto claro decifrado;

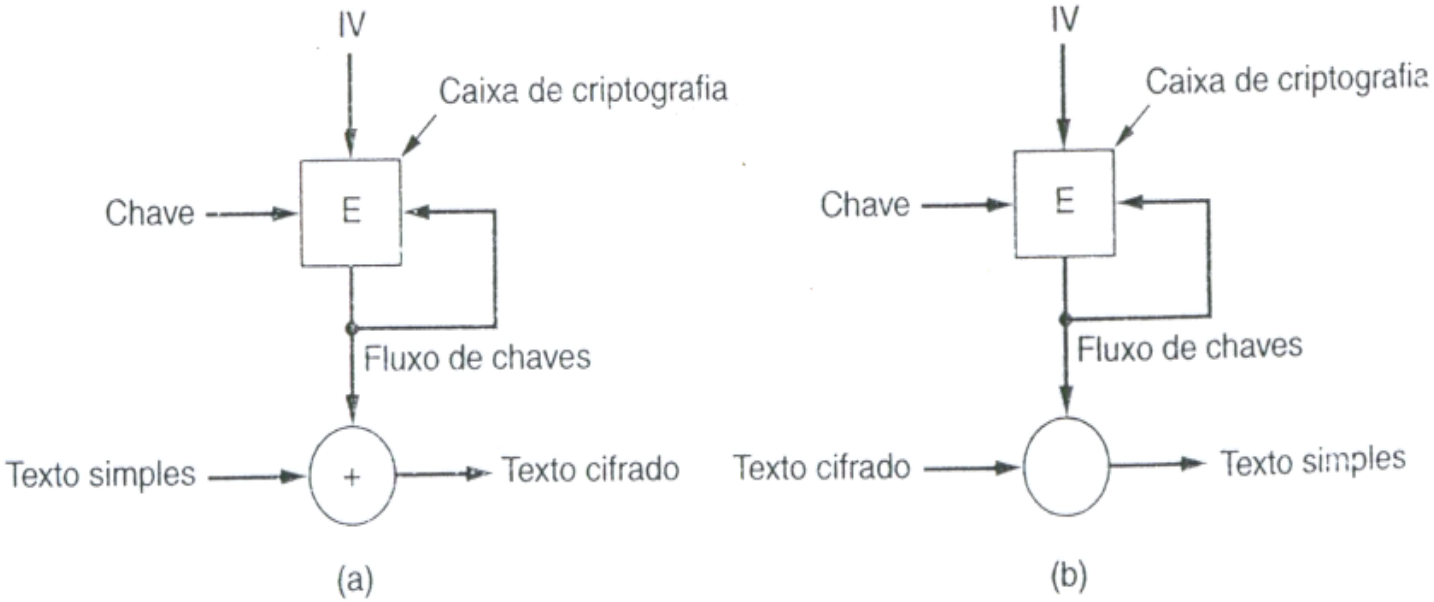


Figura 8.14 Uma cifra de fluxo. (a) Codificação. (b) Decodificação

Modos de Cifras

Cifras de Fluxo x Cifras de Bloco

- Cifradores de fluxo, tipicamente executam em uma velocidade maior que os cifradores de blocos;
- Possuem uma complexidade de hardware menor;
- Cifradores de fluxo podem ter sérios problemas de segurança, se usados incorretamente;
  - Nunca deve-se usar o mesmo IV mais de uma vez, pois isso gera o mesmo fluxo de chaves;
  - O par (IV, C) é inconveniente;

Modos de Cifras

CTR (*Counter Mode*)

- Uma limitação apresentada pelo CBC, CFB e STM (exceto o ECB) é a impossibilidade de se realizar o acesso aleatório a dados cifrados;
  - Para acessar um determinado dado, os dados anteriores deverão obrigatoriamente ser decifrados antes;
- Os arquivos de disco são acessados em ordem não-sequencial, especialmente arquivos de Bancos de Dados;
- Para sanar esta limitação foi criado o modo contador;

CTR (*Counter Mode*)

- Para sanar esta limitação foi criado o modo contador;

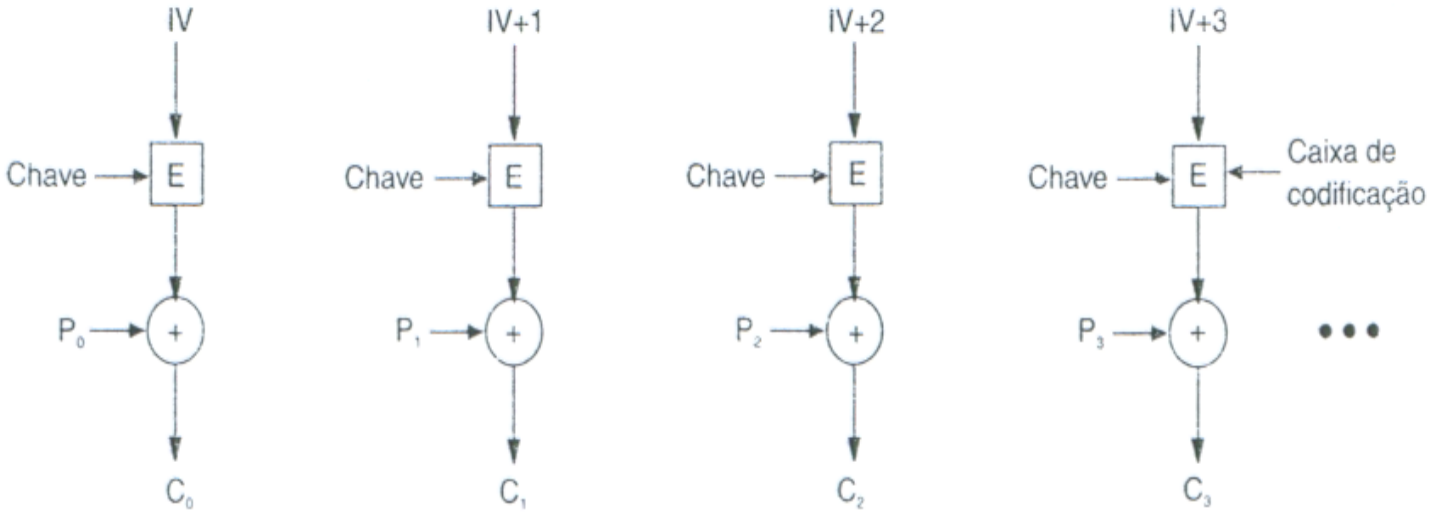


Figura 8.15 Codificação com a utilização do modo de contador

Modos de Cifras

CTR (*Counter Mode*)

- O texto claro não é codificado diretamente;
- O vetor IV é somado a uma constante inteira e cifrado;
- O texto cifrado resultante é submetido a um XOR com o texto claro;
- Aumentando-se o vetor IV em uma unidade a cada novo bloco de texto claro para ser cifrado, facilita a decifragem de um bloco em qualquer lugar no arquivo, sem que seja necessário decifrar todos os blocos predecessores;

Modos de Cifras

Exemplo com AES

- **Texto claro (21 bytes):** `testando criptografia`
- **Chave:** `computacao`
- **IV:** `91 57 69 11 3d 30 2e 78 93 cc 30 19 c5 fc 5d cb`

- **Texto cifrado (ECB – 32 bytes):**

```
5a 53 a3 cb a8 e6 11 8f 00 c6 65 fb d3 69 6a 96
84 54 23 4f ce 82 b2 b6 7b f7 d3 46 77 f8 45 34
```

- **Texto cifrado (CBC – 32 bytes):**

```
ec ff dc 8e c7 00 5f 8c 49 2f 72 af 1f 38 4d ee
45 85 7a ca bd 76 1e 45 2a 57 7d 01 1b bf 04 61
```

- **Texto cifrado (CFB – 21 bytes):**

```
19 33 3f 77 d3 97 27 3d 5b fe d3 c4 65 ca d8 70
54 ce 27 eb 03
```

Modos de Cifras

Exemplo com AES

- **Texto claro (21 bytes):** `testando criptografia`
- **Chave:** `computacao`
- **IV:** `91 57 69 11 3d 30 2e 78 93 cc 30 19 c5 fc 5d cb`

- **Texto cifrado (OFB – 21 bytes):**
  `19 54 22 a6 b8 30 66 f0 4c b9 64 7f 1b 29 f8 e3`
  `b8 f6 78 f6 00`

- **Texto cifrado (Stream com RC4 – 21 bytes):**
  `0e bc 6f d8 a8 5b 83 4c 25 47 cd 84 2a 2f 99 34`
  `68 23 e6 26 6c`