

Conceitos

A palavra “Criptografia”

Trabalhos sobre o história da criptografia

Conceito de Código

Conceito de **Cifra**

Significado da palavra “Criptografia”

A palavra **criptografia** vem das palavras gregas que significam “**escrita secreta**”.

Kriptos (em grego) = Secreto + Grafia (de escrever)

Criptografia = Escrita secreta.

Criar mensagens cifradas.

História de milhares de anos.

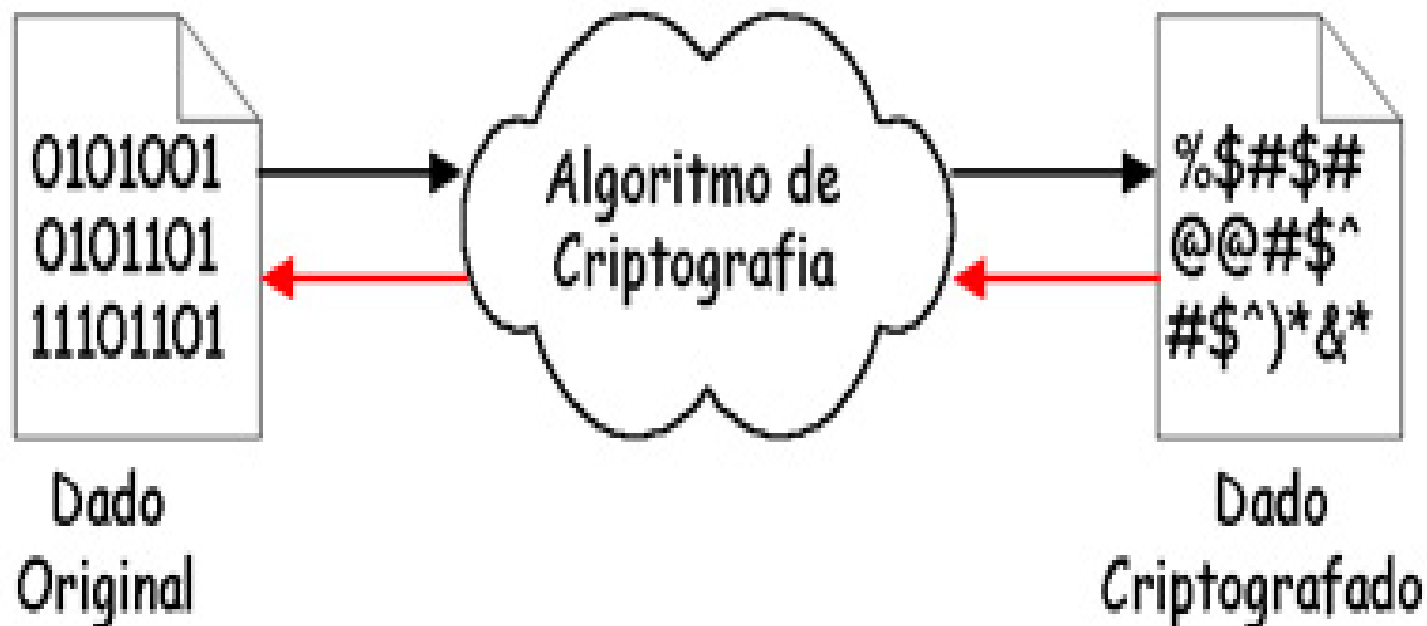
Jargões da Criptografia

Encripta (codifica, criptografa, cifra)

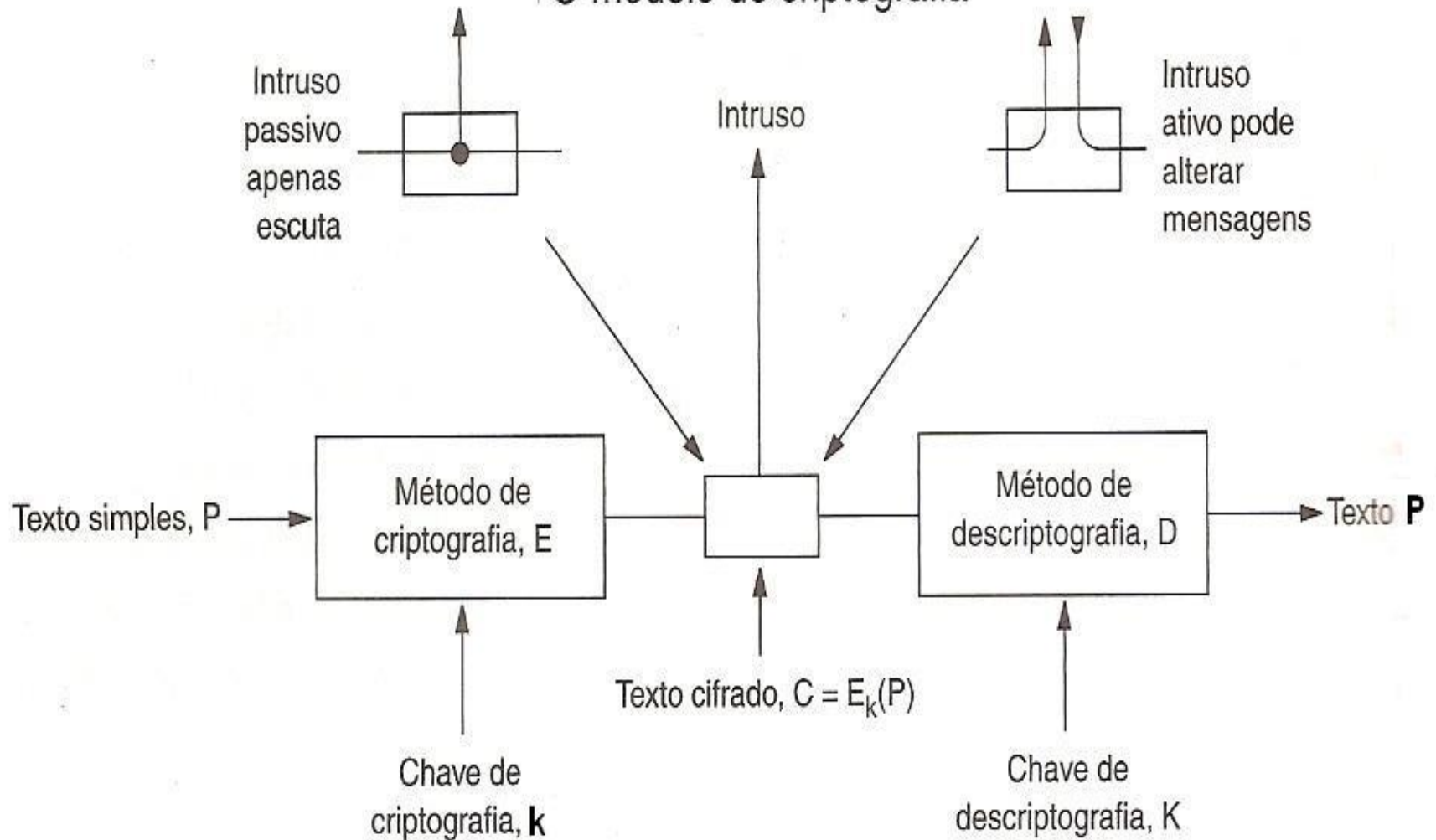
Decrypta (decodifica, decryptografa, decifra)

Procedimentos da Criptografia

Os procedimentos de **criptografar** e **decriptografar** são obtidos através de um algoritmo de criptografia.



O modelo de criptografia



Equações da Criptografia

$$D_K (E_K(P)) = P$$

E e D são funções matemáticas

K é uma **chave**

Criptografia

Possui emprego nas mais diferentes áreas de atuação, mas em todas, tem o mesmo significado:

- **proteger informações consideradas ‘especiais’ ou de qualidade sensível.**

Criptografia

Atualmente a CRIPTOGRAFIA é definida como a **ciência que oculta e/ou protege informações** – **escrita, eletrônica ou de comunicação**.

Criptografia

É o ato de **alterar** uma mensagem para esconder o significado desta.

Mas, como esconder ?

- Criando um **código** ?
- Criando **cifra** ?

Conceito de Código

Substitui uma **palavra por outra palavra** ou uma **palavra por um símbolo**.

Códigos, no sentido da criptografia, não são mais utilizados, embora tenham tido uma história ...

- O código na linguagem navajo dos índios americanos, utilizado pelos mesmos contra os japoneses na Segunda Guerra Mundial.

Conceito de Código

A **linguagem navajo** era caracterizada apenas por **sons**.

Um código é uma **transformação** que envolve somente duas **partes**.

O que é gerado chama-se uma **codificação**.

Conceito de Código

A transformação leva em conta a **estrutura linguística da mensagem** sendo transformada.

Lembre da transformação em um compilador.

Conceito de Cifra

É uma **transformação de caractere por caractere** ou **bit por bit**, **sem levar em conta** a estrutura linguística da mensagem.

Substituindo um por outro.

Transpondo a ordem dos símbolos.

Criptografia Tradicional

Historicamente, os **métodos tradicionais de criptografia** são divididos em duas categorias:

- Cifras de **Substituição**
- Cifras de **Transposição**

Cifras de Substituição

Cada **letra** ou **grupo de letras** é substituído por **outra letra** ou **grupo de letras**, de modo a criar um “disfarce”.

Exemplo: A Cifra de César (Caesar Cipher).
Considerando as 26 letras do alfabeto inglês (a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z),

Neste método, **a** se torna **d**, **b** se torna **e**, **c** se torna **f**,, **z** se torna **c**.

Generalização da Cifra de César

Cada letra se desloca k vezes, em vez de três. Neste caso, k passa a ser uma chave para o método genérico dos alfabetos deslocados de forma circular.

A Cifra de César pode enganar os cartagineses, mas nunca mais enganou a mais ninguém.

Cifras de Substituição

As cifras de substituição preservam a ordem dos símbolos no texto claro, mas disfarçam esses símbolos.

Cifras de Substituição

Cifra de César:

- cada letra é deslocada 3 vezes.

Uma ligeira generalização da Cifra de César:

- cada letra do alfabeto seja deslocada **k** vezes, em vez de 3.

Cifras de Substituição Monoalfabética

Próximo aprimoramento:

- Cada letra do texto simples, do alfabeto de 26 letras, seja mapeada para alguma outra letra.

a -> Q, b -> W, c -> E, d -> R, e -> T, ...

Esse sistema geral é chamado **cifra de substituição monoalfabética**.

Cifras de Substituição Monoalfabética

Sendo a chave uma *string* de 26 letras correspondente ao alfabeto completo.

Quebra da chave: 26! chaves possíveis.

Cifras de Substituição Monoalfabética

Um computador com o tempo de processamento de instrução de 1 ns, levaria **para quebrar essa chave** em torno de 10×10^{10} anos para experimentar todas.

Cifras de Substituição Monoalfabética

Entretanto, **apesar de parecer seguro**, com um **volume de texto cifrado surpreendentemente pequeno**, a cifra pode ser descoberta.

Estratégia: a propriedades estatísticas dos idiomas.

Cifras de Substituição Monoalfabética

Inglês: *e* é a letra mais comum, seguida de *t, o, a, n, i, ...*

Digramas mais comuns: *th, in, er, re, na, ...*

Trigramas mais comuns: *the, ing, and, ion.*

Cifras de Substituição Monoalfabética

Criptoanalista: descriptografar uma cifra monoalfabética

Conta as frequências relativas de todas as letras do texto cifrado.

Substitui com a letra e à letra mais comum e t à próxima letra mais comum.

Cifras de Substituição Monoalfabética

Em seguida, os trigramas ...

Fazendo estimativas com relação a digramas, trigramas e letras comuns ...

Cifras de Substituição Monoalfabética

e conhecendo os **prováveis padrões de vogais e consoantes**, o criptoanalista pode criar um texto simples, através de tentativas, letra por letra.

Cifras de Substituição Monoalfabética

Outra estratégia é **descobrir uma palavra ou frase provável**, a partir do conhecimento de **alguma palavra muito provável**, dentro do contexto de alguma área profissional ...

Como, por exemplo, ***financeira*** na área de contabilidade.

Cifra de Transposição

Cifras de Transposição **reordenam os símbolos**, mas **não os disfarçam**.

Exemplo: cifra de transposição de colunas.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

A cifra se baseia numa chave que é uma palavra ou uma frase que não contém letras repetidas.

Seja a chave: **MEGABUCK**

O objetivo da chave é numerar as colunas de modo que a coluna 1 fique abaixo da letra da chave mais próxima do início do alfabeto e assim por diante.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

O texto simples é escrito horizontalmente, em linhas.

O texto cifrado é lido em colunas, a partir da coluna cuja letra da chave tenha a ordem mais baixa no alfabeto.

A numeração abaixo da chave, significa a ordem das letras no alfabeto.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

M E G A B U C K

7 4 5 1 2 8 3 6

p l e a s e t r

a n s f e r o n

e m i l l i o n

d o l l a r s t

o m y s w i s s

b a n k a c c o

u n t s i x t w

o t w o a b c d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUEOERIRICXB

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

Algumas cifras de transposição aceitam um bloco de tamanho fixo como entrada e produzem um bloco de tamanho fixo como saída.

Essas cifras podem ser completamente descritas fornecendo-se uma lista que informe a ordem na qual os caracteres devem sair.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

No exemplo, a cifra pode ser vista como uma **cifra de blocos de 64 bits de entrada**.

Para a saída, a lista para a ordem de saída dos caracteres é 4, 12, 20, 28, 36, 44, 52, 60, 5, 13, ... 62.

Neste exemplo, o quarto caractere de entrada, **a**, é o primeiro a sair, seguido pelo décimo segundo, **f**, e assim por diante.

Cifra de Uso Único

Na realidade, é uma **chave de uso único** (one-time-pad).

Uma cifra inviolável, cuja técnica é conhecida há décadas.

Começa com a escolha de uma **chave de bits aleatórios**.

Cifra de Uso Único

Exemplo de como as chaves únicas são usadas:

- Seja o **texto claro 1**: *"I love you"*.
- Converter o **texto claro 1** em código ASCII.
- Escolher uma **chave 1** de bits aleatórios.
- Encontrar um **texto cifrado 1**, fazendo **XOR** entre o **texto claro 1** com a **chave 1**.

Cifra de Uso Único

Mensagem 1: 1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Chave 1: 1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Texto cifrado: 0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Chave 2: 1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Texto simples 2: 1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011

Figura 8.4 O uso de uma chave única para criptografia e a possibilidade de conseguir qualquer texto simples que seja possível a partir do texto cifrado pela utilização de alguma outra chave

Cifra de Uso Único

- Escolher outra chave, a **chave 2**, diferente da **chave 1** usada somente uma vez.
- Fazer **XOR** da **chave 2** com o **texto cifrado 1**, e encontrar, em ASCII, um possível texto claro

Cifra de Uso Único

Mensagem 1: 1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Chave 1: 1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Texto cifrado: 0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Chave 2: 1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Texto simples 2: 1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011

Figura 8.4 O uso de uma chave única para criptografia e a possibilidade de conseguir qualquer texto simples que seja possível a partir do texto cifrado pela utilização de alguma outra chave

Cifra de Uso Único

O **texto cifrado 1 não pode ser violado** porque, em uma amostra suficientemente grande de texto cifrado, **cada letra ocorrerá com a mesma frequência** (decorrente da escolha de uma chave de bits aleatórios).

O mesmo para digramas e cada trigrama.

Cifra de Uso Único

Neste exemplo, a chave única, **chave 2**, poderia ser experimentada, resultando no **texto simples 2**, “**Elvis lives**”, que está em ASCII e que pode ser ou não plausível.

Cifra de Uso Único

Isto é, todos os **textos simples 2** possíveis, com o tamanho dado, são igualmente prováveis.

De fato, para cada **texto simples 2** com código ASCII de 11 caracteres (texto simples 2), existe uma chave única que o gera.

Cifra de Uso Único

Por isso é que se diz que **não existe nenhuma informação** no texto cifrado.

É possível obter qualquer mensagem com o tamanho correto a partir dele.

Cifra de Uso Único – Imune a ataques

Esse método é imune a todos os ataques atuais e futuros, independente da capacidade computacional do intruso.

A razão deriva da Teoria da Informação:

simplesmente não existe nenhuma informação no texto simples 2.

Cifra de Uso Único – Dificuldades Práticas

As chaves únicas são ótimas na teoria, mas tem várias desvantagens na prática.

As chaves são difíceis de ser memorizadas.

Cifra de Uso Único - Dificuldades Práticas

A quantidade total de dados que podem ser transmitidos é limitada pelo tamanho da chave disponível.

Cifra de Uso Único – Dificuldades Práticas

Insensibilidade do método quanto a caracteres perdidos ou inseridos.

Se o **transmissor e o receptor ficarem sem sincronismo**, todos os caracteres a partir desse momento parecerão adulterados.

Dois princípios fundamentais da criptografia

Redundância de informação

Atualidade de mensagens

Princípio Criptográfico #1

Redundância

As mensagens criptografadas devem conter alguma redundância.

Princípio Criptográfico #2

Atualidade

Algum método é necessário para anular ataques de repetição.

O que é Redundância

São informações **não necessárias** para compreensão da mensagem clara.

Redundância

Todas as mensagens devem conter informações redundantes suficientes para que os intrusos ativos sejam impedidos de transmitir dados inválidos que possam ser interpretados como uma mensagem válida.

O que é Atualidade

Tomar algumas medidas para assegurar que cada mensagem recebida possa ser confirmada como uma mensagem atual, isto é, enviada muito recentemente.

Atualidade

Medida necessária para impedir que intrusos ativos reutilizem (repitam) mensagens antigas por intermédio de interceptação de mensagens no meio de comunicação.

Atualidade

Incluir em cada mensagem um timbre de hora válido apenas por 10 segundos.

O receptor pode manter as mensagens durante 10 segundos, para poder comparar as mensagens recém-chegadas com mensagens anteriores e assim filtrar duplicatas.

Elementos básicos de Cifras

Caixa P (Transposição é obtida por Permutação)

Caixa S (Substituição)

Cifra de Produto (Junta-se Permutações e Substituições)

Elementos básicos de Cifras

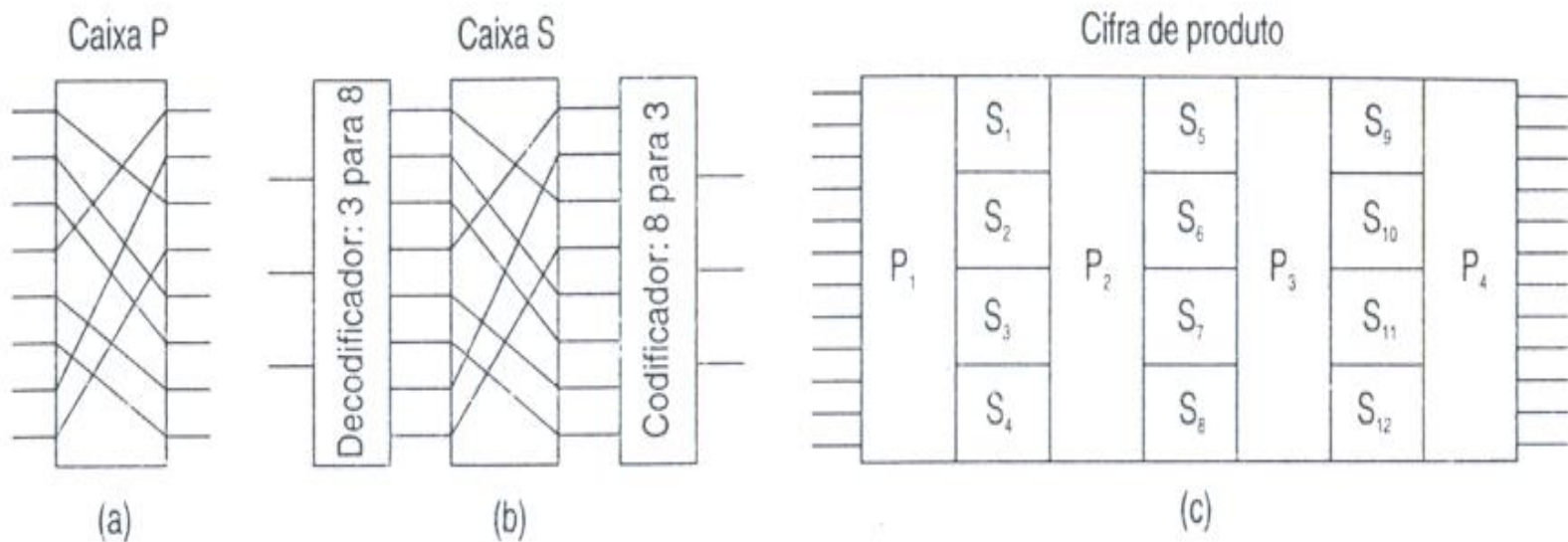


Figura 8.6 Elementos básicos de cifras de produtos.

(a) Caixa P. (b) Caixa S. (c) Produto

Modos de Cifra

Electronic Code Book – ECB

Cipher Block Chaining – CBC

Cipher FeedBack – CFB

Output FeedBack – OFB

Stream Cipher Mode – SCM (modo de cifra de fluxo)

Counter Mode – CTR (Modo de Contador)

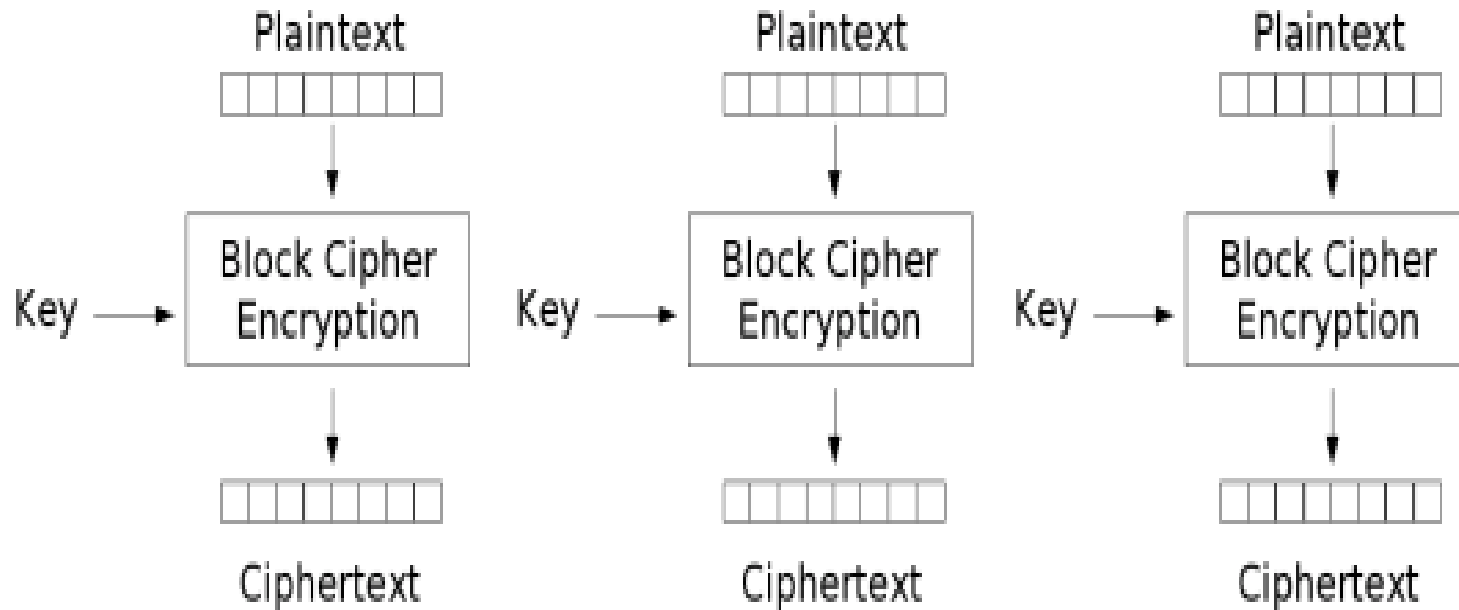
ECB – Electronic Code Book

O modo mais simples para se obter cifras.

É adequado à cifra de pequenas quantidades de dados aleatórios, como números de cartões de crédito, ou chaves utilizadas para cifrar.

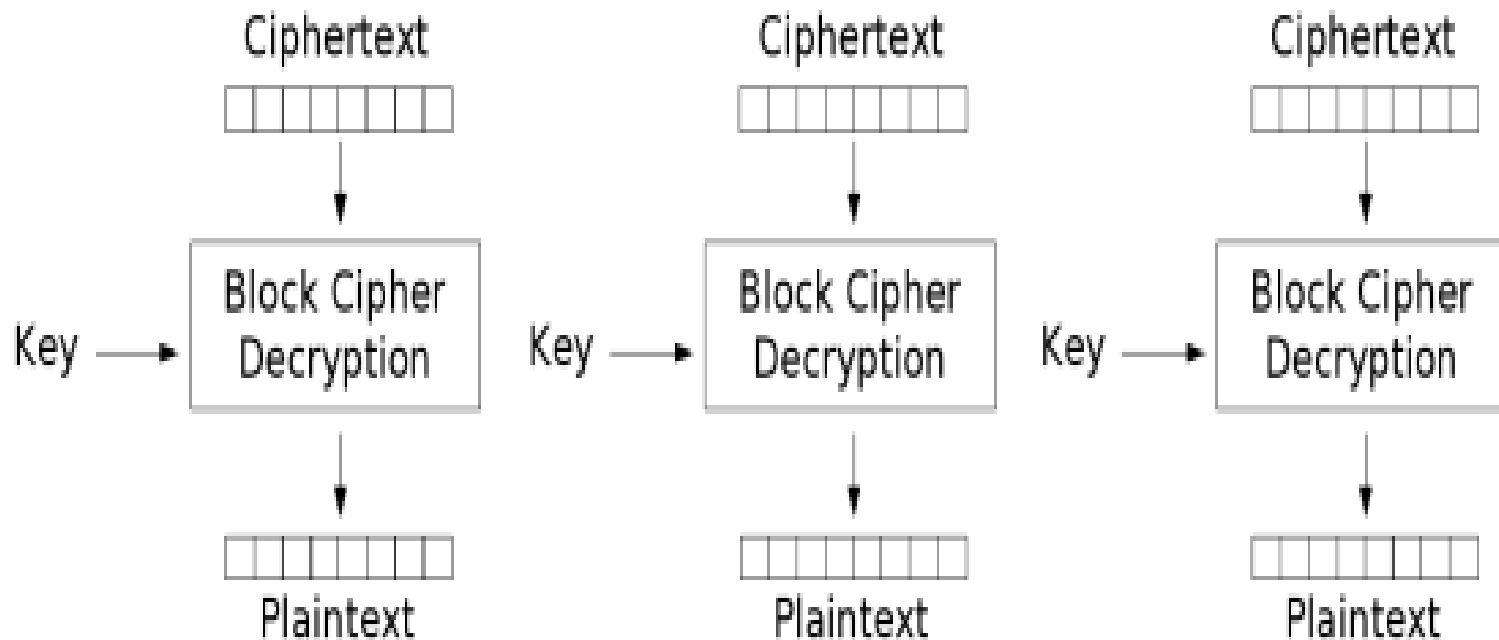
A técnica consiste em dividir a mensagem em blocos de tamanho adequado, cifrar os blocos em separado e concatenar os blocos cifrados na mesma ordem.

Electronic Code Book - ECB



Electronic Codebook (ECB) mode encryption

ECB



Electronic Codebook (ECB) mode decryption

O grande inconveniente desta técnica é que blocos de mensagem original idênticos vão produzir blocos cifrados idênticos, e isso pode não ser desejável.

Desvantagem de ECB

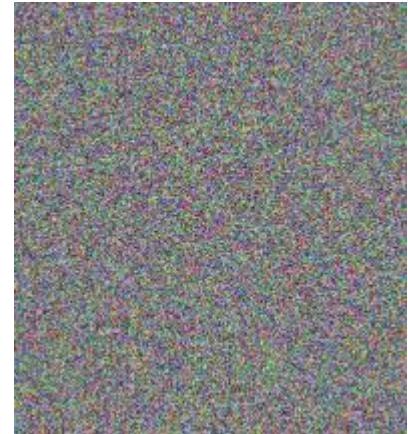
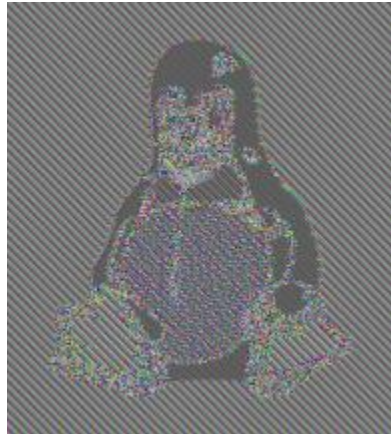
E assim, com ECB, não se pode ocultar padrões de dados.

Desvantagem com o ECB

Original



Encriptado usando outros modos



Encriptado usando modo ECB

Desvantagem de ECB

Observar que a **aparência aleatória da imagem mais à direita**, **nos diz muito pouco se a imagem foi criptografada com um método seguro**.

Muitos métodos de criptografia **inseguros** têm sido desenvolvidos, **as quais produzem saída com aspecto aleatório**.

ECB

O modo ECB produz protocolos de criptografia **sem garantia de integridade** e bastante **suscetíveis a ataques de repetição**, pois cada bloco é “descriptado” exatamente da mesma forma.


Desvantagem de ECB

No geral, não oferece uma perfeita **confidencialidade** de mensagem, e não é recomendado para uso em protocolos criptográficos em geral.

Ataque de Leslie (Tanenbaum)

| Name | | | | | | | | | | | | | | | | Position | | | | | | | | Bonus | | | | | | | |
|------|---|---|---|---|---|---|---|---|---|---|---|---|--|--|--|----------|---|---|---|---|---|---|--|-------|---|---|---|---|---|---|---|
| A | d | a | m | s | , | | L | e | s | l | i | e | | | | C | l | e | r | k | | | | \$ | | | | | | 1 | 0 |
| B | l | a | c | k | , | | R | o | b | i | n | | | | | B | o | s | s | | | | | \$ | 5 | 0 | 0 | . | 0 | 0 | 0 |
| C | o | l | l | i | n | s | , | | K | i | m | | | | | M | a | n | a | g | e | r | | \$ | 1 | 0 | 0 | . | 0 | 0 | 0 |
| D | a | v | i | s | , | | B | o | b | b | i | e | | | | J | a | n | i | t | o | r | | \$ | | | | | | | 5 |

Bytes ← 16 ← 8 ← 8 →



CBC – Cipher Block Chaining

Para contrariar esse tipo de ataque, as cifras de blocos podem ser encadeadas de várias maneiras.

Para que a substituição de um bloco como a que Leslie fez, transforme o texto simples decifrado em lixo, a partir do bloco substituído.

CBC – Cipher Block Chaining

Uma forma de encadeamento é o encadeamento de blocos de cifras
(Cipher Block Chaining).

CBC – Cipher Block Chaining

Esta técnica evita o inconveniente em ECB.

A operação **XOR** é um operador binário que compara dois bits, e então retorna 1 se os dois bits forem diferentes, ou 0 se eles forem iguais.

CBC – Cipher Block Chaining

Cada bloco de texto simples é submetido a uma operação **XOR** com o **bloco de texto cifrado anterior**, antes de ser criptografado por algum algoritmo de criptografia.

CBC – Cipher Block Chaining

Consequentemente, o mesmo bloco de texto simples não é mais mapeado para o mesmo bloco de texto cifrado.

Assim ,a criptografia não é mais uma grande cifra de substituição monoalfabética.

CBC – Cipher Block Chaining

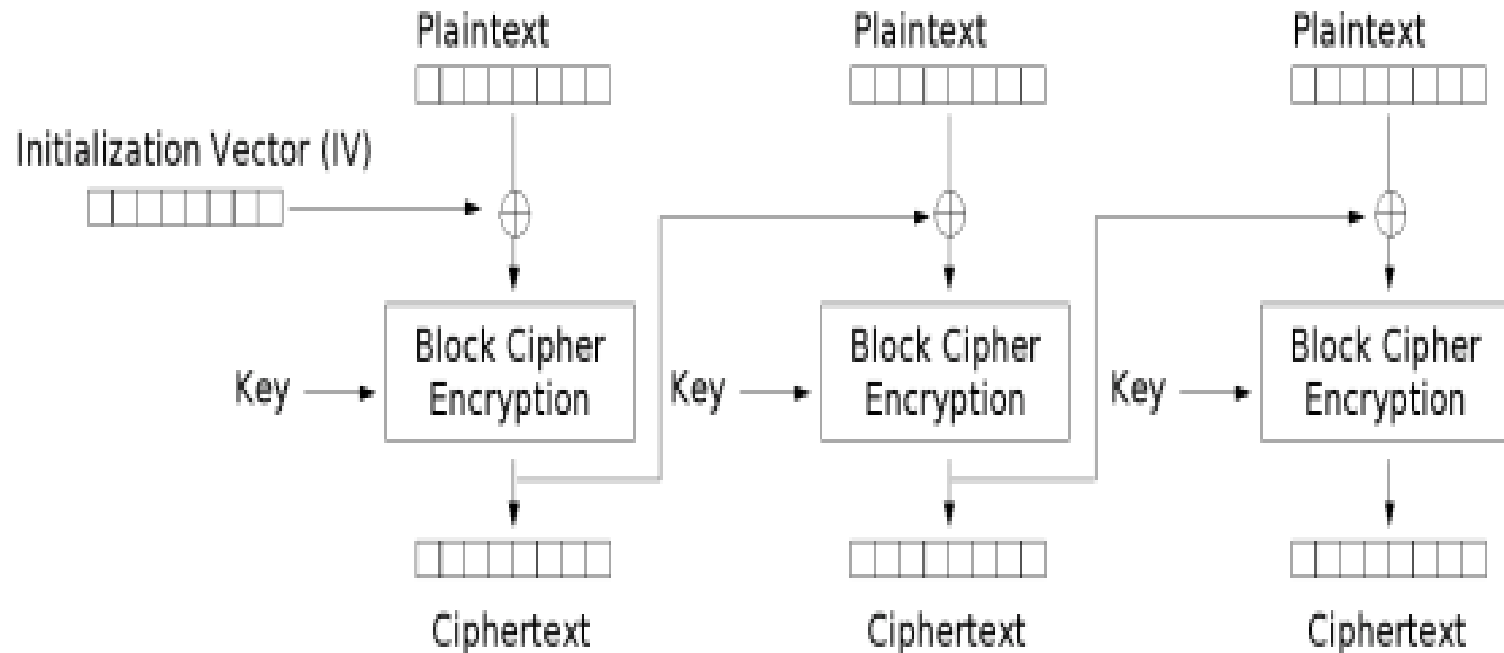
O primeiro bloco de texto simples é submetido a uma operação XOR com um vetor de inicialização IV, escolhido ao acaso, o qual tem que ser transmitido (em texto simples) juntamente com o texto cifrado.

IV – Vetor de Inicialização

Um vetor de inicialização (IV) é um meio de aumentar a segurança da cifra através da introdução de um grau de aleatoriedade.

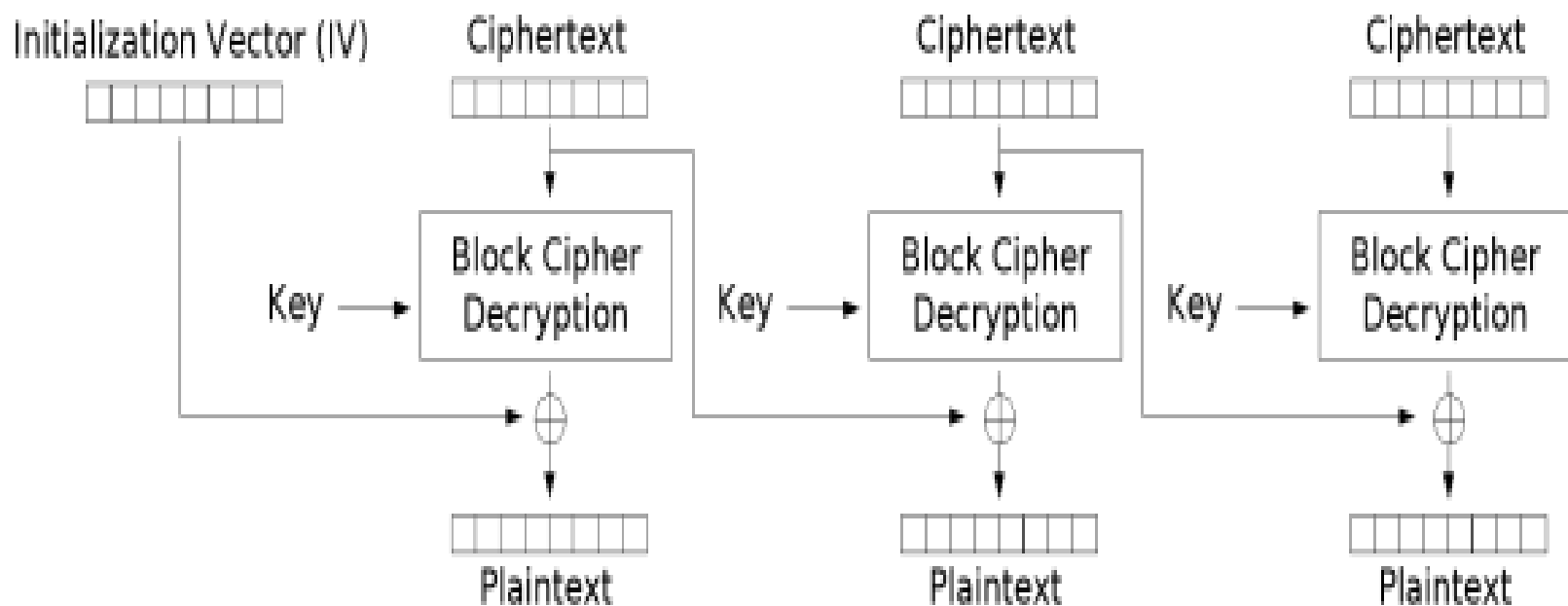
Este deve ser único, mas igual tanto na cifragem como decifragem.

CBC – Cipher Block Chaining



Cipher Block Chaining (CBC) mode encryption

CBC – Cipher Block Chaining



Cipher Block Chaining (CBC) mode decryption

CBC – Cipher Block Chaining

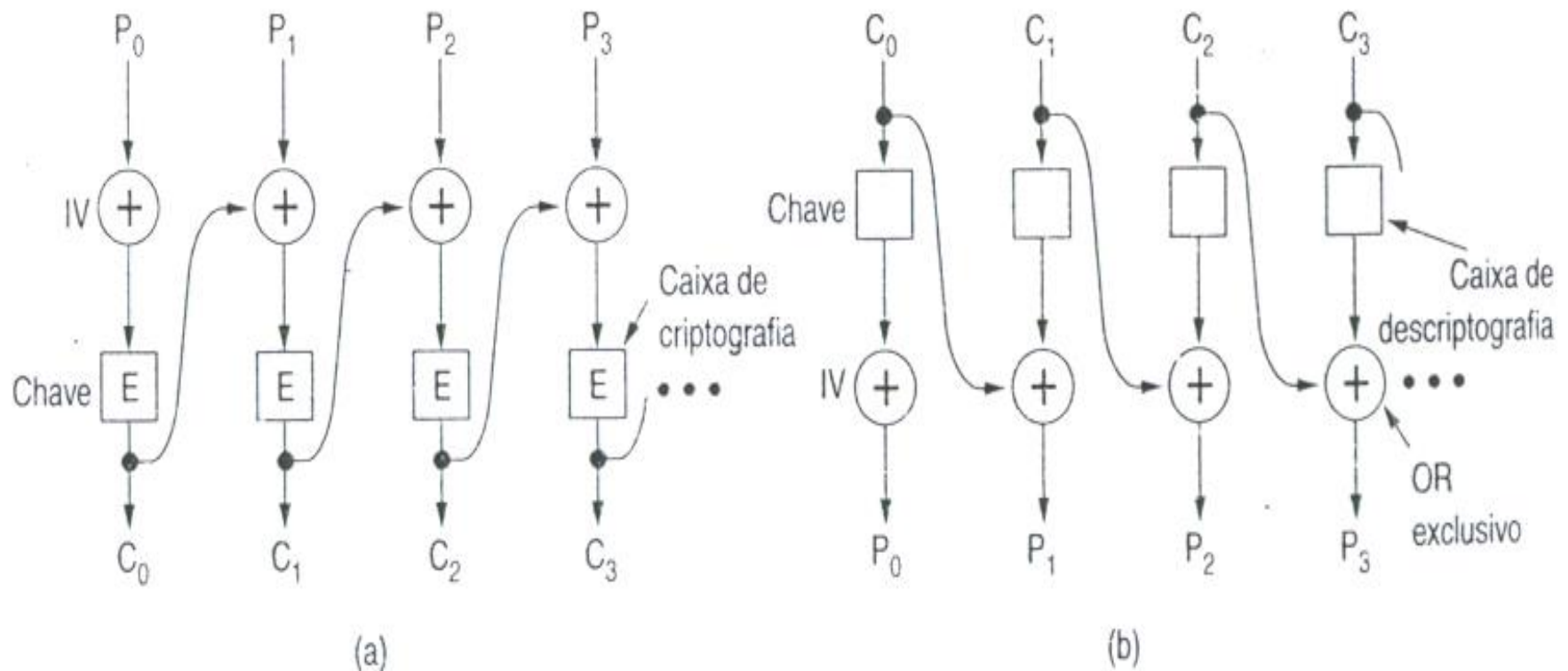


Figura 8.12 Encadeamento e blocos de cifras. (a) Codificação. (b) Decodificação

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

Criptografando CBC

$$C_0 = E(P_0 \text{ XOR } IV)$$

$$C_1 = E(P_1 \text{ XOR } C_0)$$

$$C_2 = E(P_2 \text{ XOR } C_1)$$

$$C_3 = E(P_3 \text{ XOR } C_2)$$

...

$$C_i = E(P_i \text{ XOR } C_{i-1})$$

...

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$$

Descriptografando CBC

$$P_0 = IV \text{ XOR } D(C_0)$$

$$P_1 = C_0 \text{ XOR } D(C_1)$$

$$P_2 = C_1 \text{ XOR } D(C_2)$$

...

$$P_i = C_{i-1} \text{ XOR } D(C_i)$$

...

CBC

Diferente do CBC, no ECB, a criptografia de um bloco i é uma função somente do texto simples i .

CBC

No CBC, a criptografia de um bloco i é uma função de todo texto simples contido nos blocos 0 a $i-1$.

E assim, o mesmo texto simples gera um texto cifrado diferente, dependendo de onde ele ocorre.

CBC

Uma substituição do tipo que Leslie fez **resultará em texto sem sentido para dois blocos a partir do campo da gratificação de Leslie.**

CBC

O encadeamento de blocos de cifras tem uma **vantagem**:

“o mesmo bloco de texto simples não resultará no mesmo bloco de texto cifrado”

Desvantagem em CBC

O encadeamento de blocos de cifras tem a **desvantagem** de que o processo de criptografia é sequencial e assim não pode ser paralelizado.

Desvantagem em CBC

A mensagem deve ser alinhada de acordo com um múltiplo do tamanho do bloco de cifra (64 bits ou 128 bits).

CBC

A **criptoanálise** se torna difícil.

Essa é a **principal razão de seu uso**.

O CBC é útil quando se pretende cifrar grandes quantidades de dados, como **arquivos**, apresentando **uma segurança bastante superior à do modo ECB**.

CFB – Cipher Feedback

Se por outro lado, se pretender cifrar quantidades muito pequenas de dados (bytes ou blocos pequenos) , como por exemplo, *bytes* individuais que formam um *stream* (de bytes), CFB é mais conveniente.

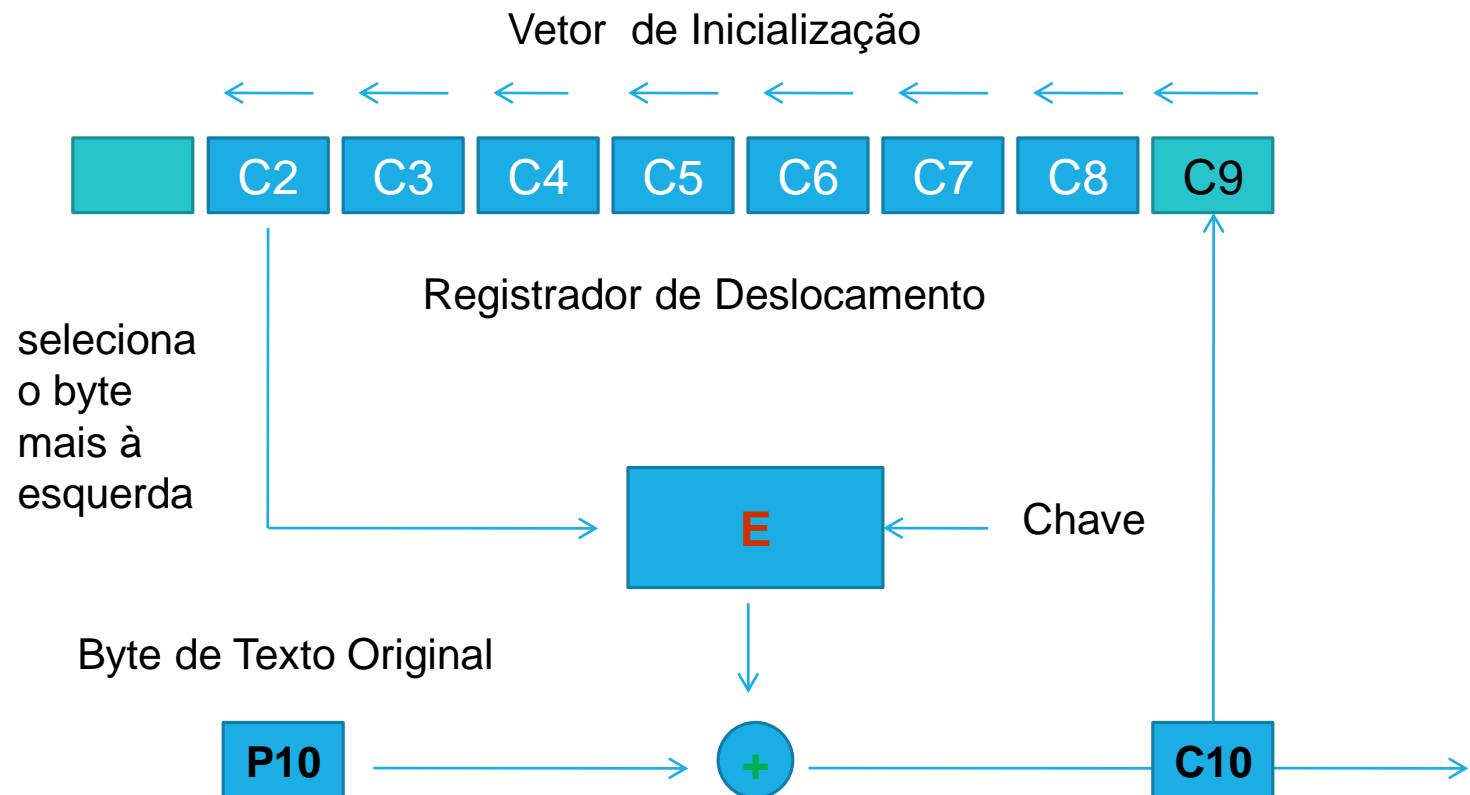
CFB

Como em CBC, é necessário um vetor de inicialização IV para dar início ao processo.

CFB

Esse vetor de inicialização funcionará como um **registrador de deslocamento R** (shift register), formado por **bytes (8 bits)** , e que pode ter um comprimento, por exemplo, de 64 bits (usando-se o DES ou 128 bits, usando o AES).

Cifragem CFB



O IV é inicializado aleatoriamente em R.

O algoritmo de criptografia (DES, AES) opera sobre o registrador de deslocamento para gerar um texto cifrado do tamanho do registrador (64 bits, 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 simples P.

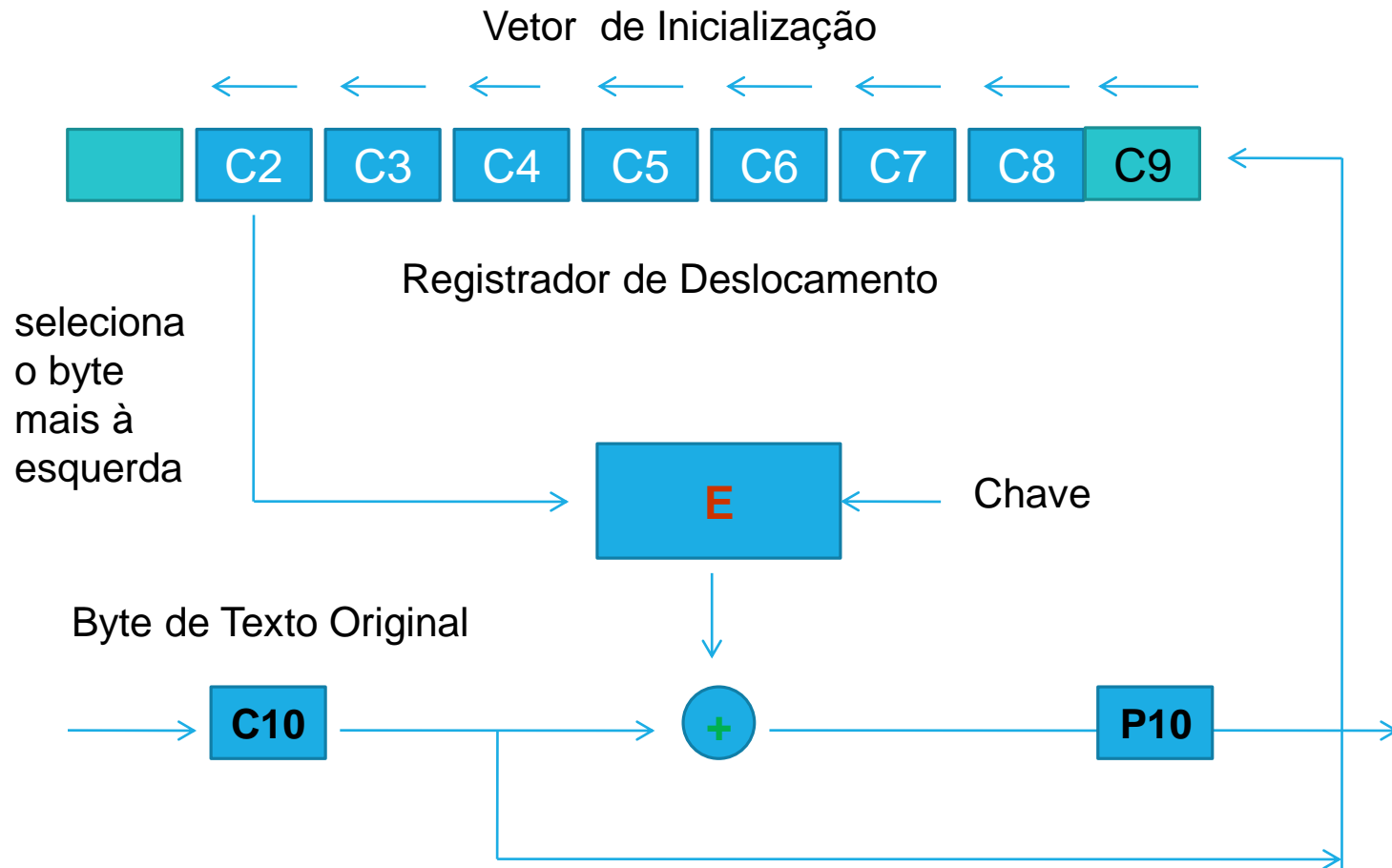
Esse byte cifrado é transmitido.

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 do XOR) seja inserido na posição que ficou vaga na extremidade do registrador mais à direita.

Observe que o conteúdo do registrador de deslocamento R depende do histórico anterior dos bytes do texto simples P .

Assim, um padrão que se repetir várias vezes no texto simples será criptografado de maneira diferente do texto cifrado a cada repetição.

Decifragem CFB



Decifragem CFB

A decifragem com o modo feedback de cifra funciona exatamente como na 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.

Decifragem CFB

E assim, o byte $C(2)$ em R, na extremidade à esquerda, cifrado em E com a chave K, e que é selecionado e submetido à **operação XOR** com o byte $C(10)$ transmitido e recebido, é o mesmo que sofreu a **operação XOR** com o byte $P(10)$ do texto simples, para gerar $C(10)$ na primeira vez.

Decifragem CFB

Desde que os dois registradores de deslocamento R (no transmissor e no receptor) permaneçam idênticos, a decifragem funcionará corretamente.

Problema no CFB

Se um bit do texto cifrado $C(10)$ 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.

Problema com CFB

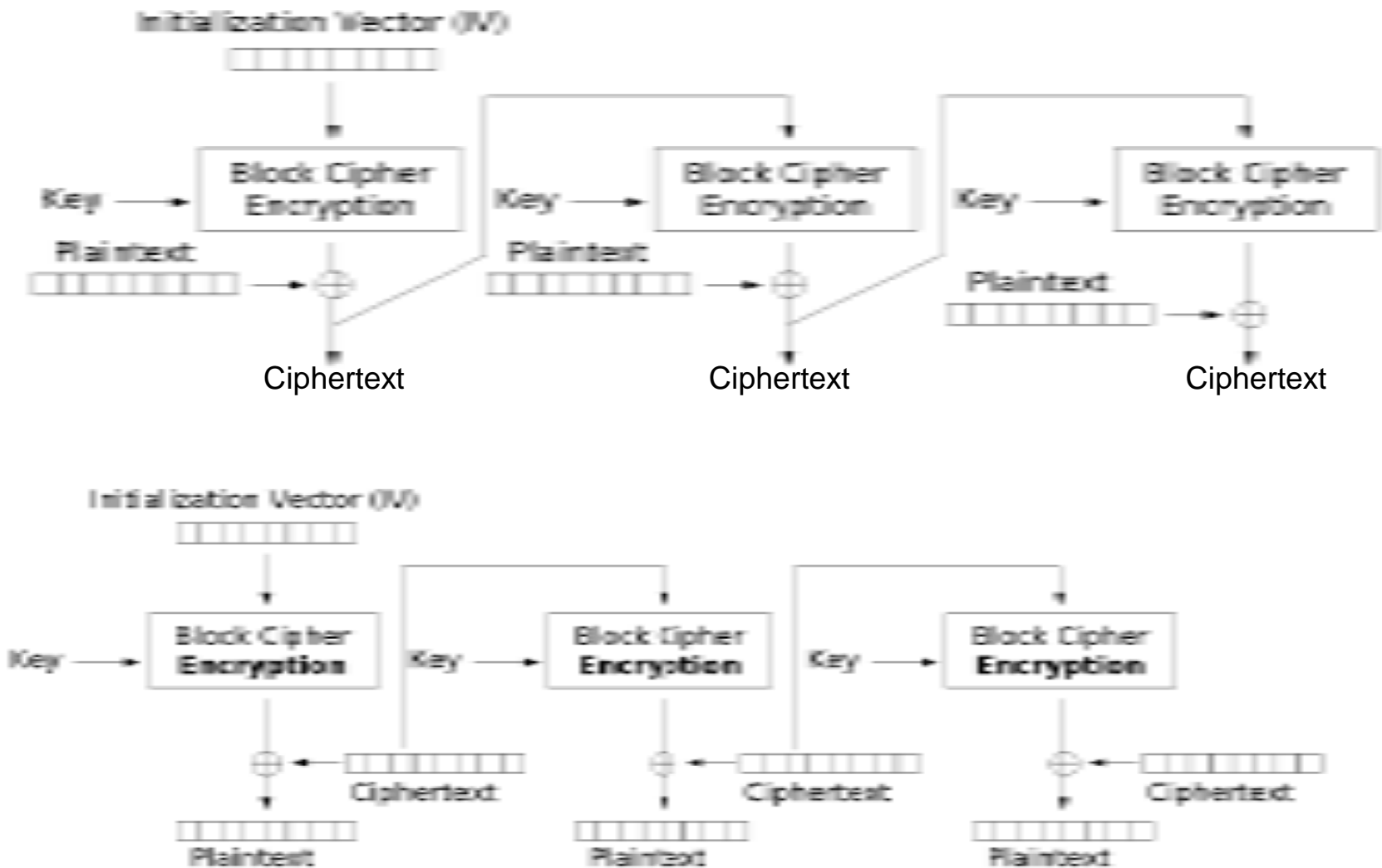
Depois que o **byte defeituoso** é empurrado para fora do **registrador** de deslocamento, o **texto simples** volta a ser gerado **corretamente** outra vez.

Problema com CFB

Deste modo, os efeitos de um único bit invertido são relativamente localizados e não arruinam o restante da mensagem.

Mas, arruinam uma quantidade de bits igual ao comprimento do registrador R de deslocamento.

CFB – Cipher FeedBack



OFB –Output Feedback

O modo OFB é análogo ao CFB, mas que pode ser utilizado em aplicações em que a propagação de erros não pode ser tolerada.

Stream Cipher

Mas, existem aplicações em que um erro de transmissão de 1 bit alterando 64 bits de texto simples provoca um impacto grande demais.

Stream Cipher

Para essas aplicações existe uma outra opção, o Modo de Cifra de Fluxo (stream cipher mode).

Funciona, inicialmente, criptografando um vetor de inicialização IV com uma chave para obter um bloco cifrado de saída.

Stream Cipher

O bloco de saída cifrado é então criptografado, usando-se a chave para obter um segundo bloco cifrado de saída.

Esse segundo bloco é criptografado com a chave para se obter um terceiro bloco cifrado de saída.

E assim por diante ...

Stream Cipher

Assim, é formada uma sequência de blocos cifrados de saída, arbitrariamente grande, de blocos cifrados de saída concatenados.

Essa sequência é chamada de **fluxo de chaves**.

Stream Cipher

A sequência formando o **fluxo de chaves** é tratada como **uma chave única** e submetida a uma **operação XOR com o texto simples**.

Stream Cipher

Observe que o **fluxo de chaves** formado é independente dos dados (texto simples), e portanto, pode ser calculado com antecedência, se necessário.

O **fluxo de chaves** é completamente insensível (não sujeito) a erros de transmissão.

Decifrando STC

A decifragem ocorre gerando-se o mesmo fluxo de chaves no lado do 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.

Decifragem STC

Desse modo, um erro de 1 bit no texto cifrado transmitido gera apenas um erro de 1 bit no texto simples decifrado.

Cifrando e Decifrando em STC

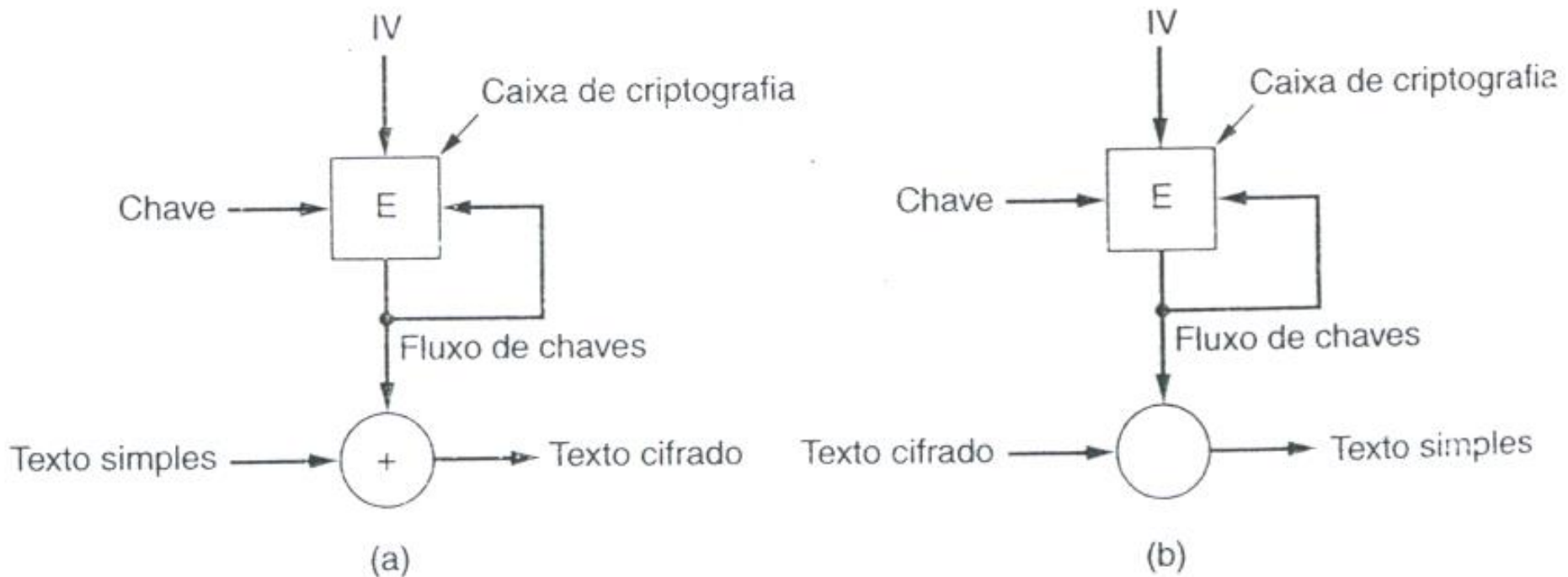


Figura 8.14 Uma cifra de fluxo. (a) Codificação. (b) Decodificação

Stream Cipher X Block Cipher

Cifradores de fluxo, tipicamente, executam em uma velocidade maior que os cifradores de bloco.

Têm uma complexidade de Hardware menor.

Problemas de Segurança

Contudo, cifradores de fluxo podem ser susceptíveis a sérios problemas de segurança, se usados incorretamente.

Problemas de Segurança

É essencial nunca se usar o IV duas vezes ou mais, pois isso irá gerar o mesmo fluxo de chaves C , o tempo todo.

O par (IV, C) é inconveniente.

Problemas de Segurança

O uso de um mesmo fluxo de chaves C , duas vezes, expõe o texto cifrado a um ataque de reutilização do fluxo de chaves C .

Um ataque em STC

Sejam A e B mensagens do mesmo comprimento, ambas criptografadas usando-se a mesma chave C.

$$E(A) = A \text{ xor } C$$

$$E(B) = B \text{ xor } C$$

Se um adversário capturar $E(A)$ e $E(B)$, ele pode facilmente computar:

$$E(A) \text{ xor } E(B).$$

Um ataque em STC

Contudo, xor é uma operação comutativa e também $X \text{ xor } X = 0$.

$$\begin{aligned}\text{Assim, } E(A) \text{ xor } E(B) &= \\ &= (A \text{ xor } C) \text{ xor } (B \text{ xor } C) = \\ &= (A \text{ xor } B) \text{ xor } C \text{ xor } C = \\ &= (A \text{ xor } B) \text{ xor } 0 \\ &= A \text{ xor } B \text{ o que elimina a chave } C.\end{aligned}$$

Um ataque em STC

Agora o atacante tem um XOR dos dois textos simples A e B transmitidos.

Se um deles for conhecido ou puder ser encontrado, o outro também poderá ser encontrado.

Um ataque em STC

Em todo caso, o XOR de dois textos simples poderá ser atacado com o uso de propriedades estatísticas sobre um dos textos.

Em resumo, equipado com o XOR de dois textos simples, o criptoanalista tem uma excelente chance de deduzí-los.

Aplicação de Stream Cipher

Um cifrador de fluxo (A5/1) utilizado para prover comunicação privada em GSM é baseado num registrador de deslocamento à esquerda (LFSR) e tem uma operação para gerar um fluxo de chaves usado para criptografar conversações em telefones móveis.

CTR - Counter Mode

Um problema apresentado por CBC, CFB, STC, execto ECB, é a impossibilidade de conseguir acesso aleatório a dados codificados.

Os arquivos de disco são acessados em ordem não-sequencial, especialmente arquivos de BDs.

CTR

No caso de um arquivo codificado pela utilização do encadeamento de blocos de cifras (CBC), o acesso a um bloco aleatório exige primeiro a decifragem de todos os seus blocos anteriores, ou seja um proposta dispendiosa.

CTR

Esta a razão de se criar um modo contador.

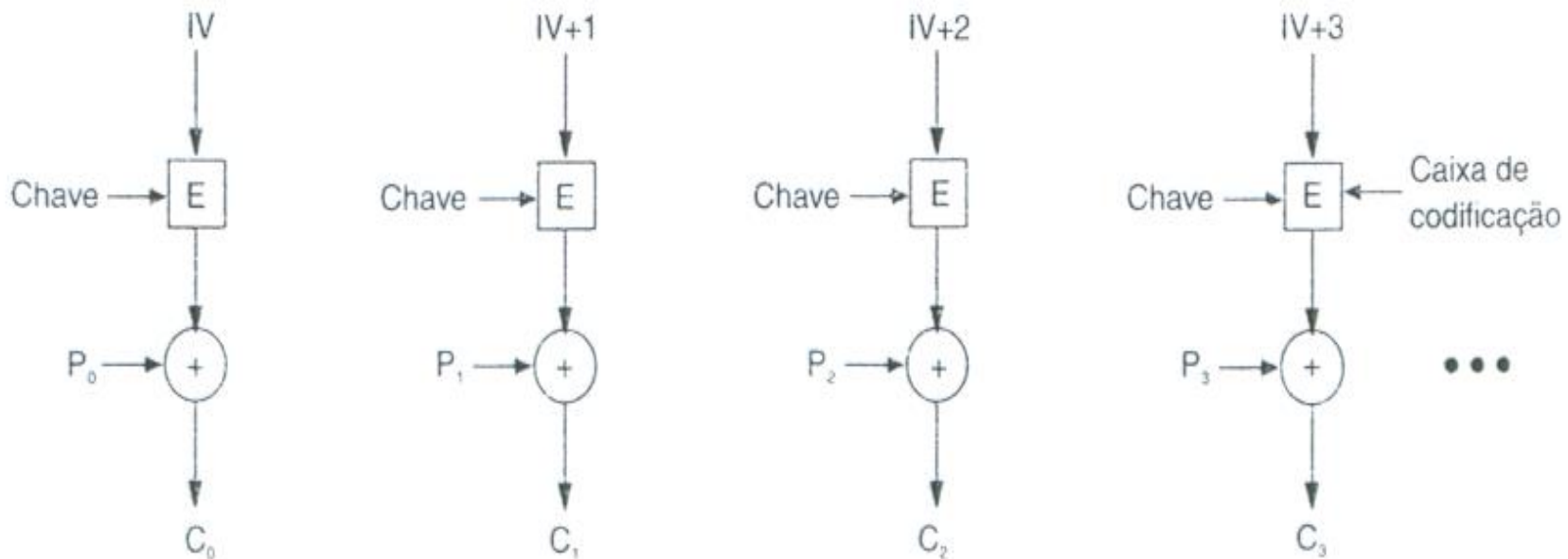


Figura 8.15 Codificação com a utilização do modo de contador

CTR

O texto simples 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 simples.

CTR

Aumentando-se o vetor IV em uma unidade a cada novo bloco do texto simples para ser cifrado, facilita a decifragem de um bloco em qualquer lugar no arquivo, sem que seja preciso, primeiro, decifrar todos os seus blocos predecessores.

Trabalhos sobre o História da Criptografia

Histórico completo (Khan, 1995)

Estado da arte em segurança e protocolos criptográficos (Kaufman et al., 2002)

Abordagem mais matemática (Stinson, 2002)

Abordagem menos matemática (Burnett e Paine (2001)

Estrutura de Estudo

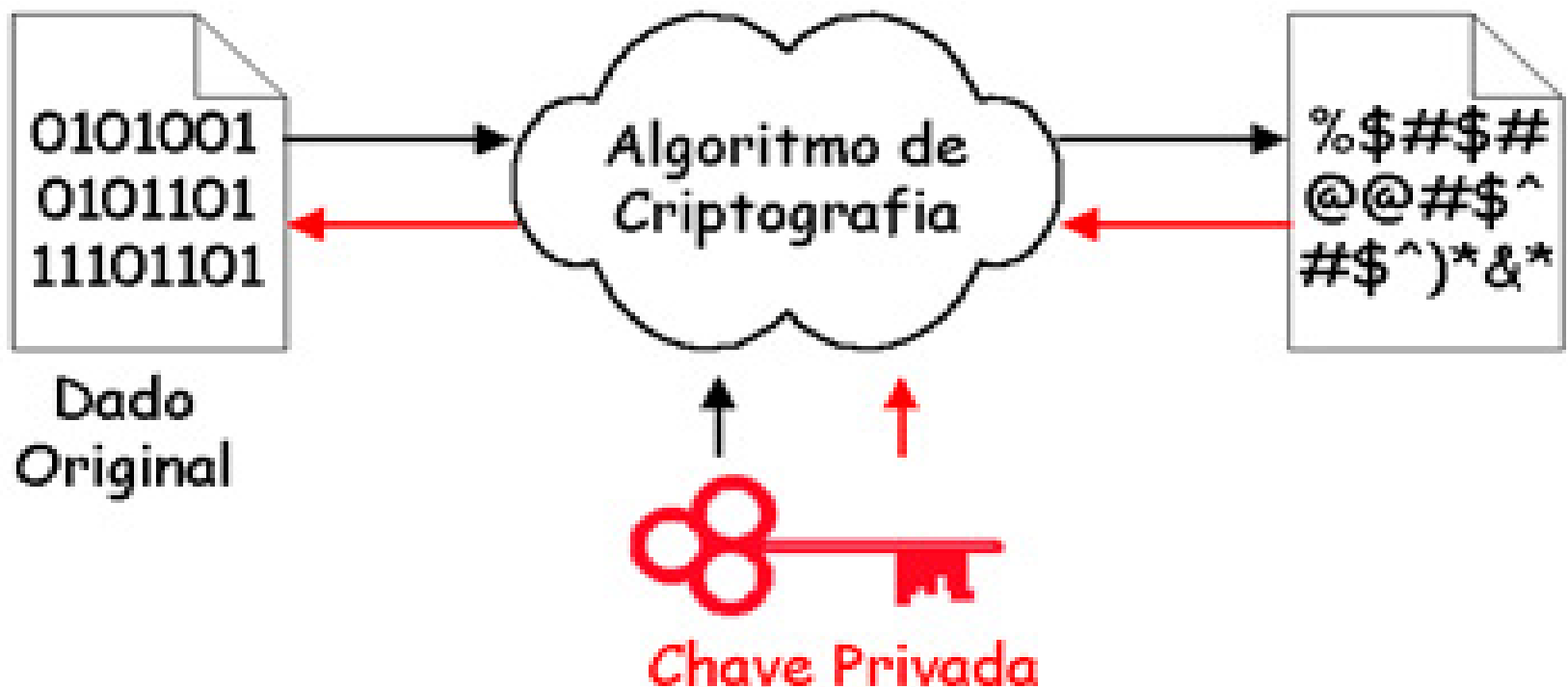
**CRIPTOGRAFIA E SEGURANÇA DA
INFORMAÇÃO**

Técnicas envolvendo criptografia

Garantia de Confidencialidade

Garantia de Privacidade

Criptografia Simétrica

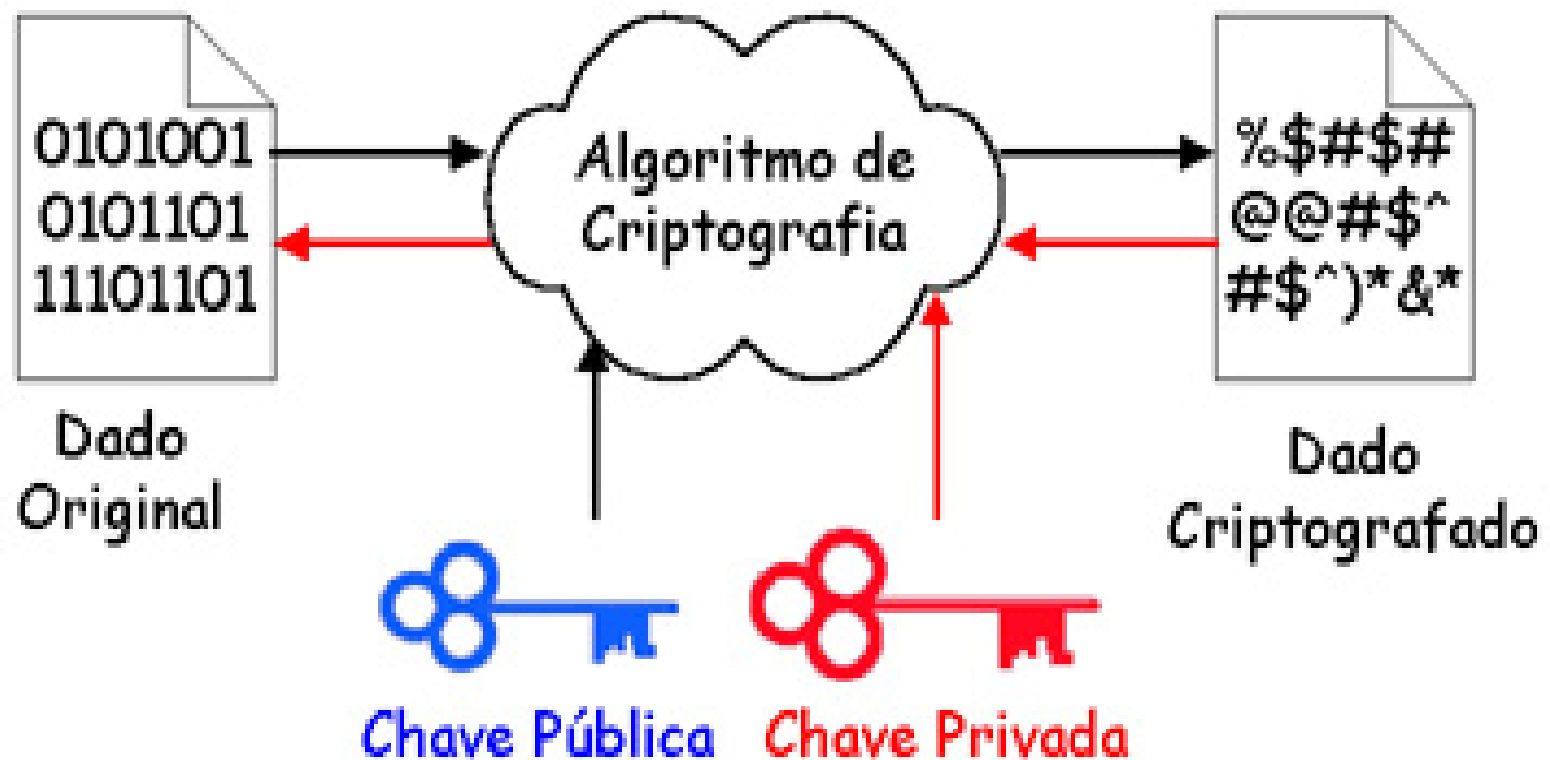


Técnicas envolvendo criptografia simétrica

Algoritmos de Criptografia de **Chave Simétrica**,

Gerenciamento de Chaves Simétricas,

Criptografia Assimétrica



Técnicas envolvendo criptografia de chave pública

Algoritmos de Criptografia de Chaves Públicas

O problema de **distribuição de chaves**

Infra-estrutura de chaves públicas

Técnicas envolvendo criptografia

Mas, se não houver preocupação com sigilo da informação ...

Ou o desempenho da criptografia de chave pública é imprescindível.

Resumos de Mensagem

Uma **forma mais rápida de criptografia** (simétrica ou assimétrica).

Um **representante dos dados**.

Garantia de **Integridade**

Algoritmos **Hash**

Problema

Mas, a **mensagem** e o **resumo** são preparadas e transmitidas em separado, **um intruso pode capturar a mensagem e também pode capturar o resumo** correspondente.

Duas maneiras de resolver o problema

Utilizar uma **assinatura digital**.

Uma **chave-resumo (HMAC)**, resume a chave e os dados, **nesta ordem**.

Códigos de Autenticação de Mensagem

Resolvem o problema de se transmitir mensagem e resumo, **não mais separadamente**.

HMAC

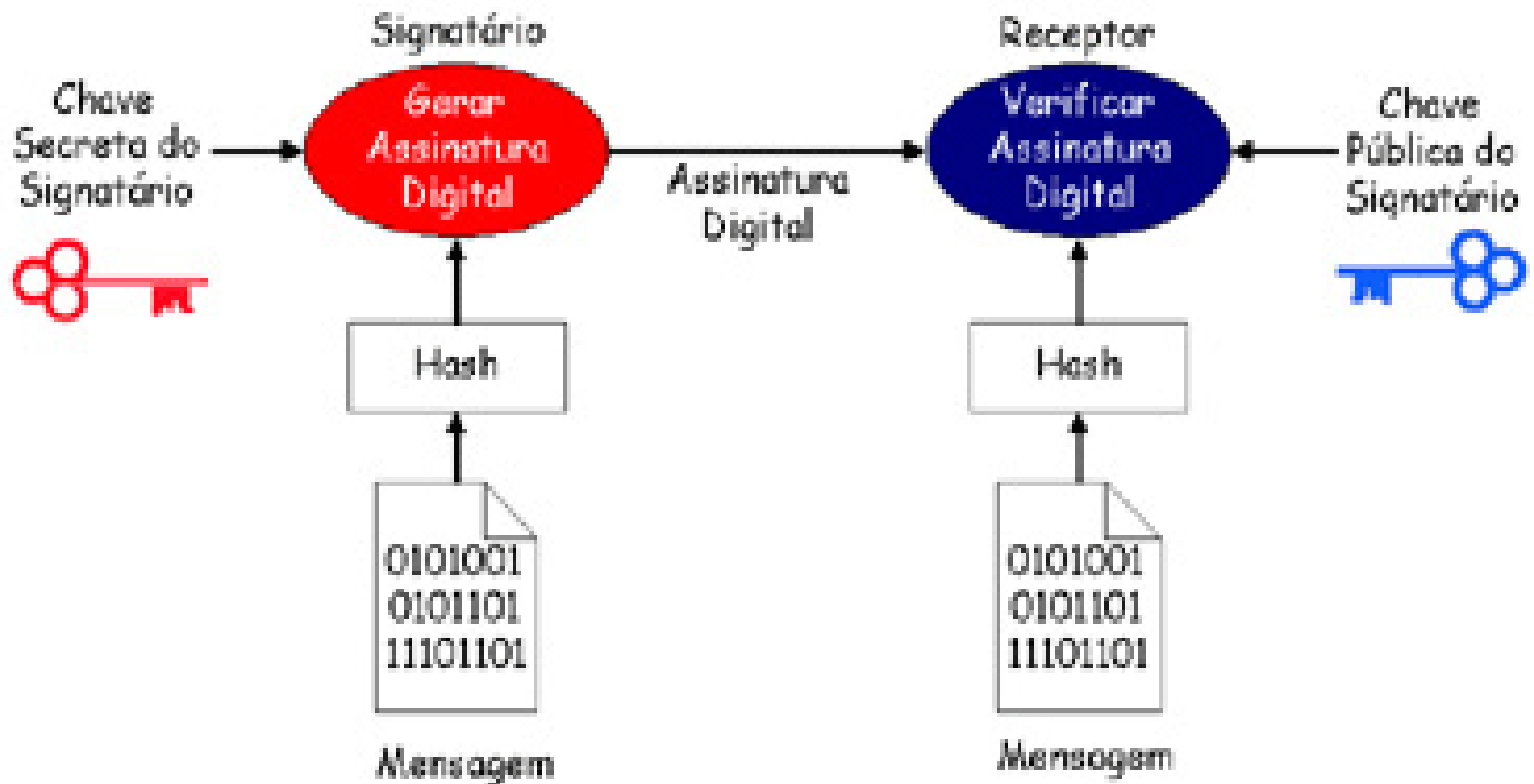
São utilizadas apenas para verificar se o conteúdo não foi alterado durante o trânsito.

É uma verificação instantânea e não um registro permanente.

Assinaturas Verificáveis

Por essa razão, **necessitamos de uma outra maneira de criar assinaturas verificáveis** e essa maneira é **encriptar o resumo com a chave privada do assinante** (que é o que se chama de assinatura digital).

Assinatura Digital



Assinatura Digital

Garantia de **Autenticidade**

Garantia de **Integridade**

Garantia de **Não-Repúdio**

Problema com as assinaturas

Assinaturas são suficientes num número limitado de pessoas, quando as pessoas, de certa forma, se conhecem.

Quando alguém tem que verificar uma assinatura, deve obter a chave pública do remetente da mensagem.

Problema com as assinaturas

Como o destinatário da mensagem pode ter certeza de que a chave pública recebida é de fato o dono da chave pública quando enviou a mensagem ?

Uma solução ...

Servidor on-line de chaves públicas na Internet 24 horas ?

On-Line ?

Replicação de servidores ?

Certificados Digitais

Técnicas envolvendo criptografia

PROTOCOLOS COM CRIPTOGRAFIA

Segurança nas Camadas

Com exceção da **segurança na camada física**, quase **toda segurança se baseia em princípios criptográficos**.

Criptografia de Enlace

Na camada de enlace, os quadros em uma linha ponto-a-ponto podem ser codificados, à medida que saem de uma máquina, e decodificados quando chegam em outra.

Criptografia de Enlace

Vários detalhes de criptografia **poderiam ser tratados na camada de enlace**, no entanto, **essa solução se mostra ineficiente, quando existem vários roteadores.**

Criptografia de Enlace

Pois é necessário decriptar os pacotes, em cada roteador, o que pode tornar esses, **vulneráveis a ataques dentro do roteador**.

Também, algumas sessões de aplicações são protegidas, mas outras, não.

Criptografia na Camada de Rede

A segurança do **Protocolo IP** funciona nesta camada.

Estudar o **Protocolo IPSec**

Criptografia na Camada de Transporte

É possível criptografar conexões fim-a-fim, ou seja processo-a-processo.

SSL (Security Socket Level)

TLS (transport Level Security)

Stunnel para criptografia com **protocolos não SSL** (por exemplo, **SSH**)

Criptografia na Camada da Aplicação

S/MIME (**S**ecure/**M**ultipurpose Internet **M**ail **E**xtensions)

SET (Secure Electronic Transactions)

HTTPS (HTTP sobre SSL)

Criptografia na Camada da Aplicação

Autenticação de usuários

Não-Repúdio

Só podem ser tratadas na camada da aplicação.

Uma aplicação da Criptografia Simétrica

Segurança de Bancos de Dados Oracle

Apenas as pessoas apropriadas podem ter acesso às informações no BD (**autenticação de usuários**).

Os **dados precisam ser protegidos** e uma maneira de proteger os dados é por **criptografia**.

Segurança de Bancos de Dados Oracle

Geração da Chave:

Alguns **bytes aleatórios** ou **pseudo-aleatórios** são gerados e utilizados como uma **chave** para a criptografia simétrica DES ou TripleDES.

Segurança de Bancos de Dados Oracle

Armazenamento da Chave:

Precisa-se também **salvar essa chave gerada em algum lugar** (não no mesmo lugar onde foi gerada). O próximo capítulo ensina como armazenar a **chave simétrica**.

Criptografando em um BD Oracle

A chave é usada para criptografia ...

```
dbms obfuscation toolkit.DESEncrypt (  
  inputstring => plaintext,  
  key => keydata,  
  encrypted string => ciphertex );
```

Decriptografando em um BD Oracle

A chave é recuperada e ...

```
dbms obfuscation toolkit.DESDecrypt (  
  inputstring => ciphertex,  
  key => keydata,  
  encrypted string => plaintext );
```

Utilidades na Segurança da Informação

Utilidades na Segurança da Informação

Segurança e Privacidade em um Navegador.

Segurança de Emails.

Criptografia de Diretórios, Subdiretórios Arquivos.

Transferência de Arquivos.

Garantindo os requisitos de segurança

Confidencialidade

Privacidade

Autenticidade

Integridade

Não-Repúdio