Cifras de Bloco

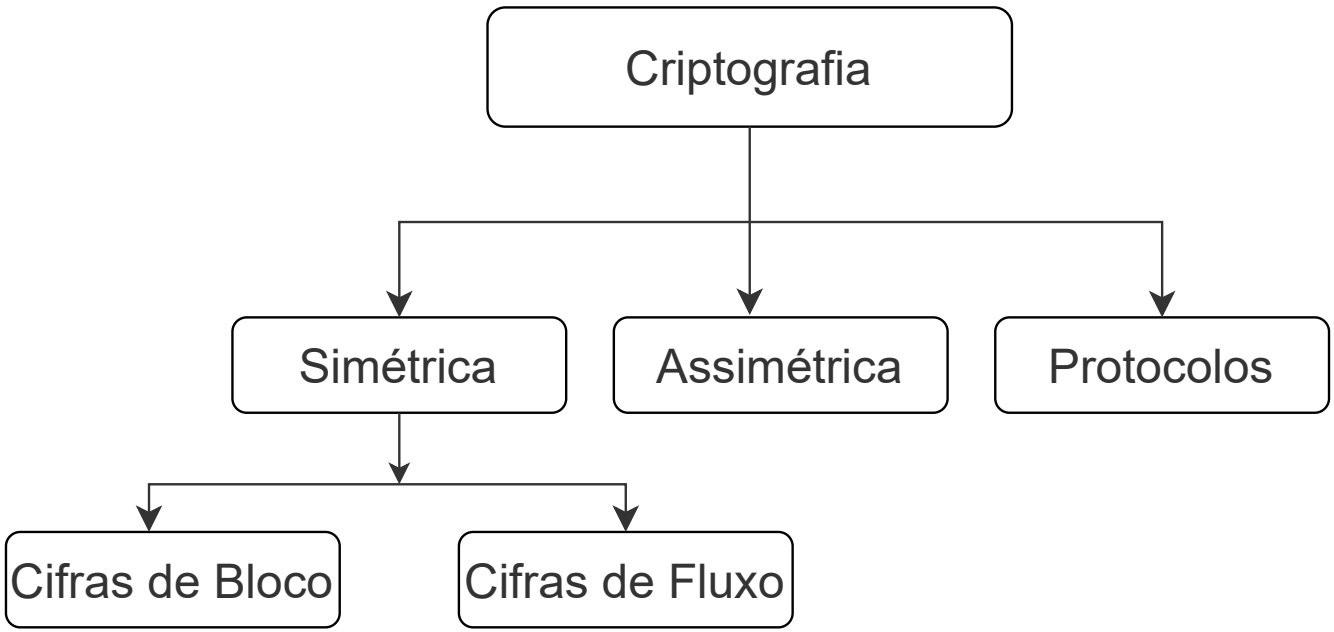
Auditoria e Segurança de SI

Prof. Roberto Cabral
rbcabral@ufc.br

Universidade Federal do Ceará

1º semestre/2023

Introdução


Criptografia
Simétrica
Assimétrica
Protocolos
Cifras de Bloco
Cifras de Fluxo

Cifras de bloco

- Encriptam um bloco inteiro do texto claro com uma mesma chave.
- Nessas cifras, a encriptação de qualquer bit de um dado bloco depende de todos os outros bits desse bloco.
- Na prática, a grande maioria das cifras de blocos possuem blocos de 128 bits.

Cifra DES

- O algoritmo de cifra de blocos DES (*Data Encryption Standard*) encripta blocos de 64 bits.
- Foi desenvolvido pela IBM sob influência da NSA (*National Security Agency*) e não teve seus critérios de projetos revelados.
- É baseado na cifra *Lucifer*.
- Foi padronizado pelo NBS (*National Bureau of Standard*), hoje chamado de NIST (*National Institute of Standard and Technology*).

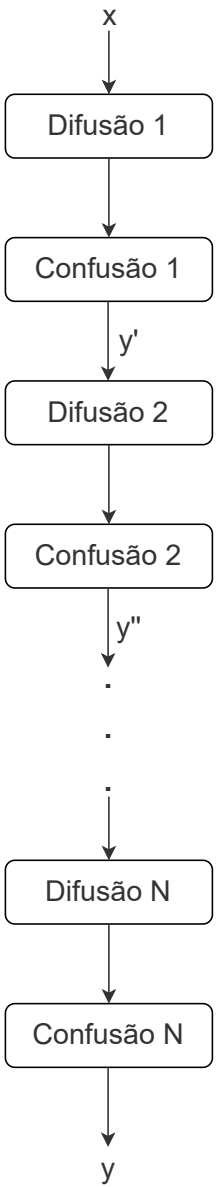
Cifra DES

- Foi a cifra mais popular por mais de 30 anos.
- De longe o algoritmo simétrico mais estudado.
- Hoje em dia é considerado inseguro, visto que possui uma chave de 56 bits.
- Mas existe uma versão conhecida como 3DES que continua segura hoje e em dia e é ainda amplamente utilizada.
- Foi substituído pelo AES (*Advanced Encryption Standard*) em 2000.

Confusão e Difusão

- Shannon: existem duas operações primitivas sobre as quais algoritmos criptográficos fortes podem ser criados:
  1. Confusão: Uma operação criptográfica onde a relação entre a chave e o texto encriptado é obscurecido.
  2. Difusão: Uma operação de criptografia onde a influência de um símbolo de texto claro é espalhada por muitos símbolos de texto encriptado com o objetivo de ocultar as propriedades estatísticas do texto claro.
- As duas operações individualmente não conseguem prover segurança! A ideia é concatenar elementos de confusão e difusão para construir uma cifra mais poderosa, conhecida como `cifra de produto`.

Cifra de produto



- A maioria das cifras de bloco são cifras de produto e consistem de várias rodadas que são aplicadas repetidamente sobre os dados.
- Podemos atingir uma excelente difusão: a substituição de um simples bit do texto claro resulta, na média, na troca de metade dos bits de saída.
- Exemplo:

DES

- O DES usa uma rede de Feistel
  - Vantagem: o processo de encriptação e decriptaçao são iguais, mudando apenas a geração de chaves.
- O algoritmo tem uma permutação inicial e então é processa 16 rodadas:
  - O texto claro é dividido ao meio, L_i e R_i.
  - R_i, juntamente com a chave K_i alimentam a função f.
  - É feito um XOR com a saída da função f e L_i.
  - A metade esquerda é trocada pela metade direita.
- As rodadas podem ser expressas por:
  - $L_i = R_{i-1}$.
  - $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$.

Segurança do DES

- As principais crítica feitas ao algoritmo DES foram:
  - O espaço de chaves é muito pequeno, deixando o algoritmo vulnerável a ataques de força bruta.
  - Os critérios usados na escolha do S-boxes foram mantidos em segredo. Desse modo, poderia existir algum ataque analítico que explora alguma propriedade matemática dos S-boxes que seria conhecido apenas pelos projetistas do DES.

Historia dos Ataque no DES

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Ano	Proposta/Implementação do Ataque
1977	Diffie & Hellman, (sub-)estimaram o custo de uma máquina de busca de chaves
1990	E. Biham e A. Shamir propuseram *criptoanálise diferencial*, que requer 2^{47} escolhas de textos claro.
1993	M. Matsui propôs *criptoanálise linear*, que requer 2^{43} escolhas de textos encriptados.
Jun. 1997	*DES Challenge I* - esforço distribuído na internet levou 4,5 meses
Fev. 1998	*DES Challenge II* - A fundação Electronic Frontier criou a máquina de pesquisa de chaves por cerca de US $250.000. O ataque levou 56 h (média de 15 dias)
Jan. 1999	*DES Challenge III* - ataque usando a máquina de pesquisa de chaves juntamente com a internet levou 22 horas
Abr. 2006	As universidades da Bochum e Kiel criaram a máquina de busca de chaves com base em FPGAs de baixo custo por aproximadamente US $ 10.000. O tempo médio de pesquisa é de 7 dias.

Implementação em Software do DES

- Uma implementação direta do DES, provavelmente resultará em um desempenho muito ruim.
- Muitas das operações do DES envolvem permutações de bits, que é muito lento em software.
- O uso de pequenos S-boxes, como os usados no DES, são eficientes em hardware, mas não tem eficientes em software.
- Uma técnica de implementação que já foi bastante usada para acelerar a computação do DES foi usar tabelas com valores pré-computados de várias operações DES.
- Uma técnica muito interessante foi proposta por Eli Biham em 1997 (*bit slicing*). Sua principal limitação é a necessidade de processar vários blocos por vez.

Implementação em Hardware do DES

- O DES foi projetado para ser muito eficiente em Hardware.
- Os S-boxes pequenos também são relativamente fáceis de serem implementados em hardware.
- Uma implementação eficiente em termos de área de uma simples rodada do DES pode ser feita com menos de 3000 portas.

Advanced Encryption Standard (2001, NITS)

- História:
  - Concurso público.
  - Foram submetidos 21 algoritmos e 15 foram aceitos.
  - 5 finalistas: MARC, RC6, Rijndael, Serpent e Twofish.
  - A cifra Rijndael foi escolhida como padrão.
- Critérios
  - Segurança
  - Custo computacional em software e hardware.
  - Simplicidade e flexibilidade no projeto.

Advanced Encryption Standard (2001, NITS)

- O algoritmo *Advanced Encryption Standard* (AES) foi publicado pelo NIST em 2001.
- AES é um cifrador de bloco que encripta uma mensagem M de 128 bits usando uma chave k e produz um texto encriptado C de 128 bits.
- O tamanho da chave pode ser de 128, 192 ou 256 bits.
- O cifrador AES é denotado por AES-128, AES-192 ou AES-256 dependendo do tamanho da chave usada.

Advanced Encryption Standard (2001, NITS)

- A cifra AES recebe como entrada uma mensagem a ser encriptada M e uma chave k.
- A mensagem M é tratada como um `estado` de 128 bits, que pode ser visto como uma matriz S de 4×4 bytes.
- O AES modifica o estado iterativamente usando um conjunto de operações, onde o número de iterações N depende do tamanho da chave.
- O estado é modificado a cada rodada pelas seguintes transformações:
  - `SubBytes`.
  - `ShiftRows`.
  - `MixColumns`.
  - `AddRoundKey`.

Cifras de Bloco

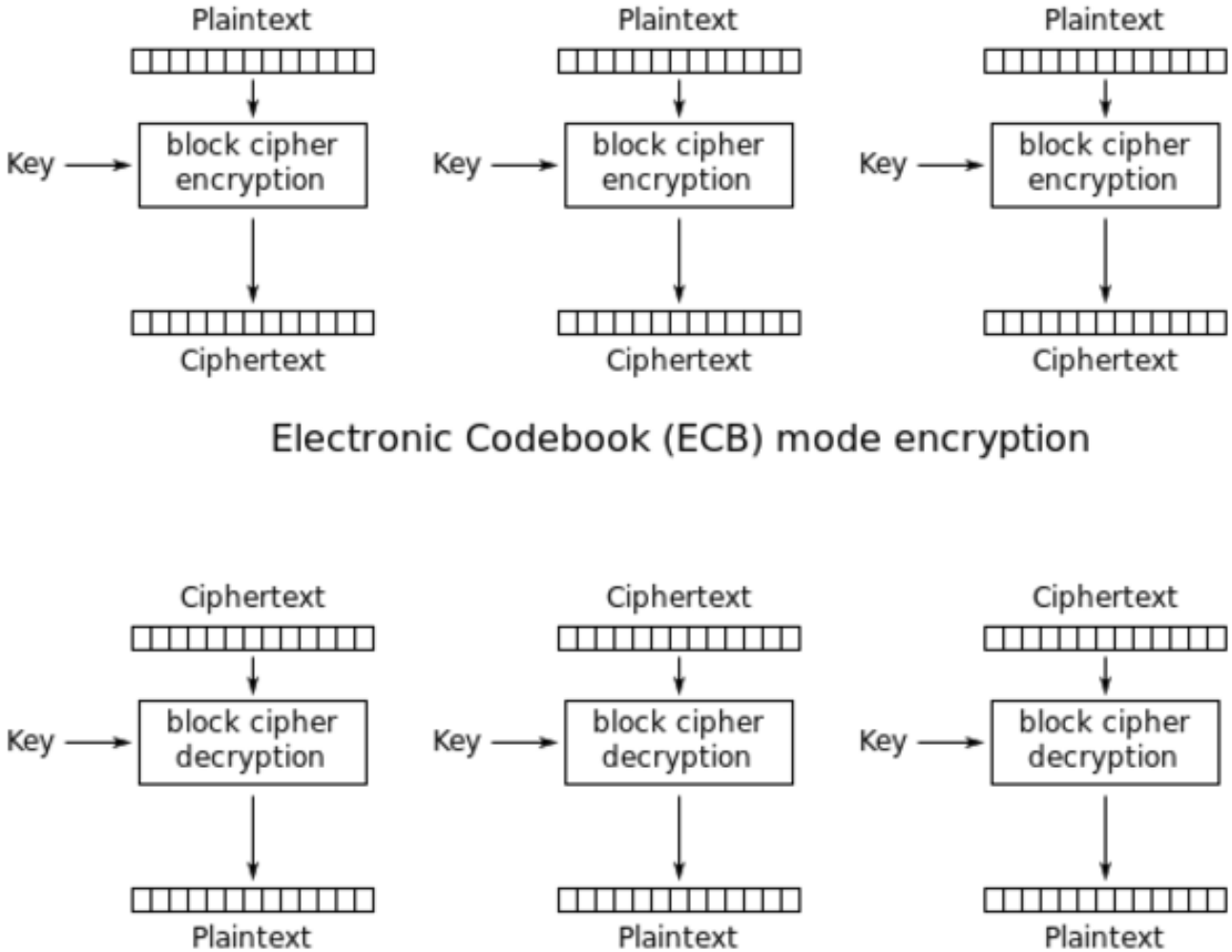
- Uma cifra de bloco é bem mais que um simples algoritmo de encriptação, ela pode ser usada para:
  - Construir diferentes tipos de esquemas baseados em encriptação baseada em blocos.
  - Realizar cifras de fluxo.
  - Construir funções de resumo.
  - Construir Códigos Autenticadores de Mensagens.
  - Construir protocolos de estabelecimento de chaves.
  - Gerar números pseudoaleatórios
  - ...
- A segurança de uma cifra de bloco pode ser incrementada por:
  - *key whitening*.
  - Encriptação múltipla.

Encriptação com Cifras de bloco

- Existem várias maneiras de encriptar textos claros longos, por exemplo, um e-mail ou um arquivo de computador, com uma cifra de bloco ("modos de operação").
  - *Electronic Code Book mode* (ECB)
  - *Cipher Block Chaining mode* (CBC)
  - *Output Feedback mode* (OFB)
  - *Cipher Feedback mode* (CFB)
  - *Counter mode* (CTR)
  - *Galois Counter Mode* (GCM)
- Todos os seis modos possuem um objetivo:
  - Além de confidencialidade, alguns fornecem autenticidade e integridade.
    - A mensagem realmente vem do remetente original? (autenticidade)
    - O texto encriptado foi alterado durante a transmissão? (integridade)

Electronic Code Book mode (ECB)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ



Vantagens e Desvantagens

- Vantagens:
  - Não é necessário sincronização de blocos entre o remetente e o receptor.
  - Os erros de bit causados por canais ruidosos só afetam o correspondente bloco, mas não afetam os blocos seguintes.
  - O funcionamento da cifra do bloco pode ser paralelizado
    - Implementações mais eficientes.
- Desvantagens:
  - A encriptação do ECB é determinística.
    - Textos claros idênticos resultam em textos encriptados idênticos.
    - Um invasor reconhece se a mesma mensagem foi enviada duas vezes.
    - Os blocos de texto claro são encriptados independentemente dos blocos anteriores
    - Um atacante pode reordenar blocos de textos encriptados que resultem em textos claros válidos.

Ataque de substituição no ECB

- Uma vez que um mapeamento entre textos claros e textos encriptados é conhecido $x_i \rightarrow y_i$, uma sequência de textos encriptados podem ser facilmente manipuladas.
- Suponha uma transferência bancária online:

Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

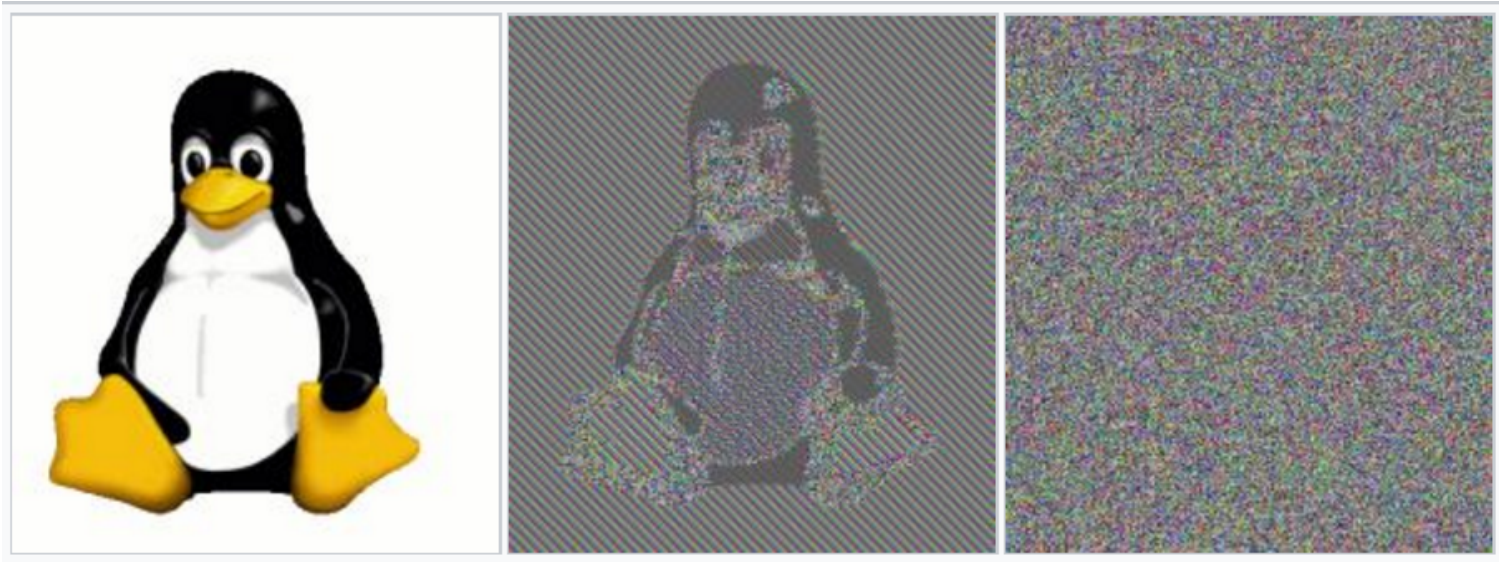
- A chave de encriptação entre dois bancos não é mudada frequentemente.
- O atacante faz transferência de R$ 1,00 de sua conta em um banco A para sua conta em um banco B repetidamente.
  - Ele pode verificar os blocos de textos encriptados que se repetem e guardar os blocos 1, 3 e 4 dessas transferências.

Ataque de substituição no ECB

- O atacante pode, simplesmente, trocar o bloco 4 de outras transferências com o bloco 4 que ele armazenou previamente.
  - Todas transferências entre contas do banco A para o banco B serão redirecionadas para a conta do atacante no banco B.

Exemplo de encriptação de mapa de bits no ECB

- Textos claros idênticos mapeiam no mesmo texto encriptado.

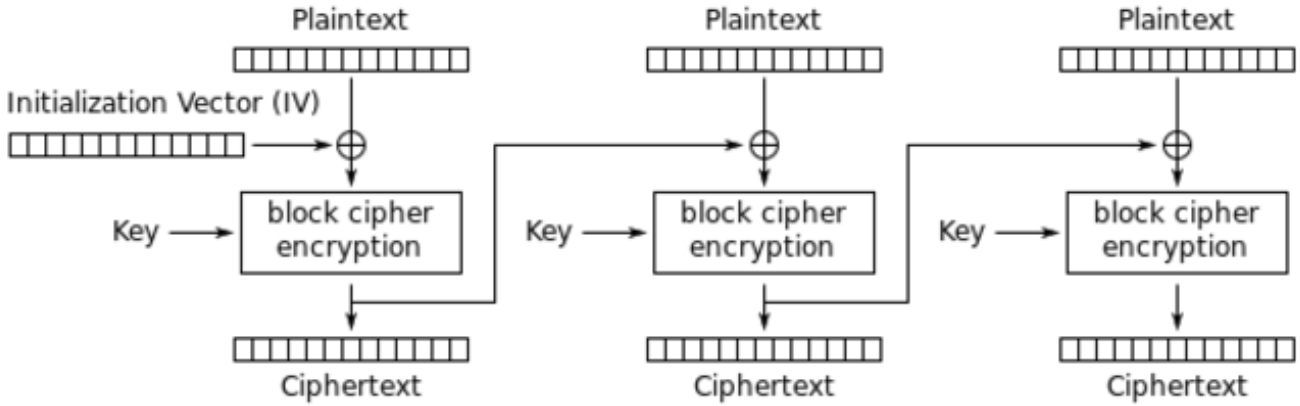


Original image | Encrypted using ECB mode | Modes other than ECB result in pseudo-randomness

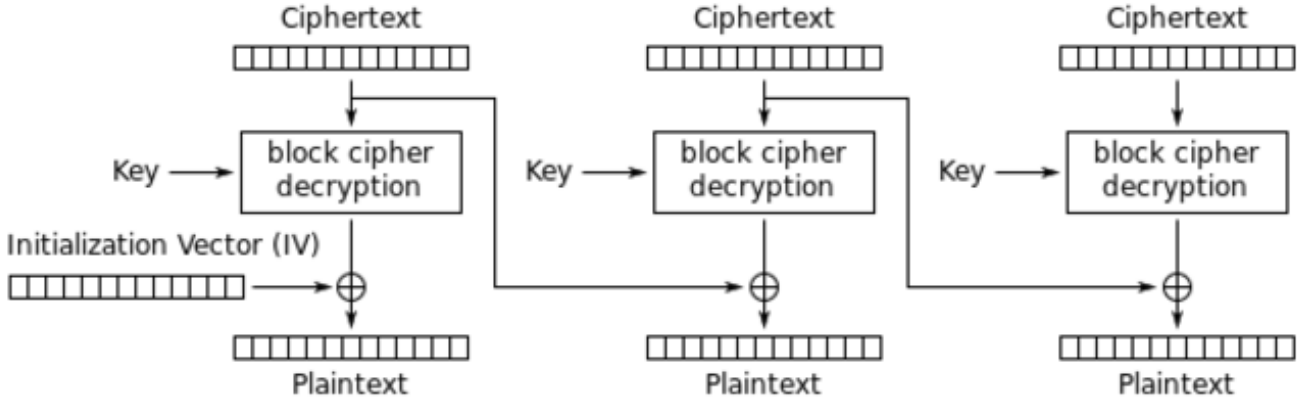
- Propriedades estatísticas do texto claro são preservadas no texto encriptado.

Cipher Block Chaining mode (CBC)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ



Cipher Block Chaining (CBC) mode encryption



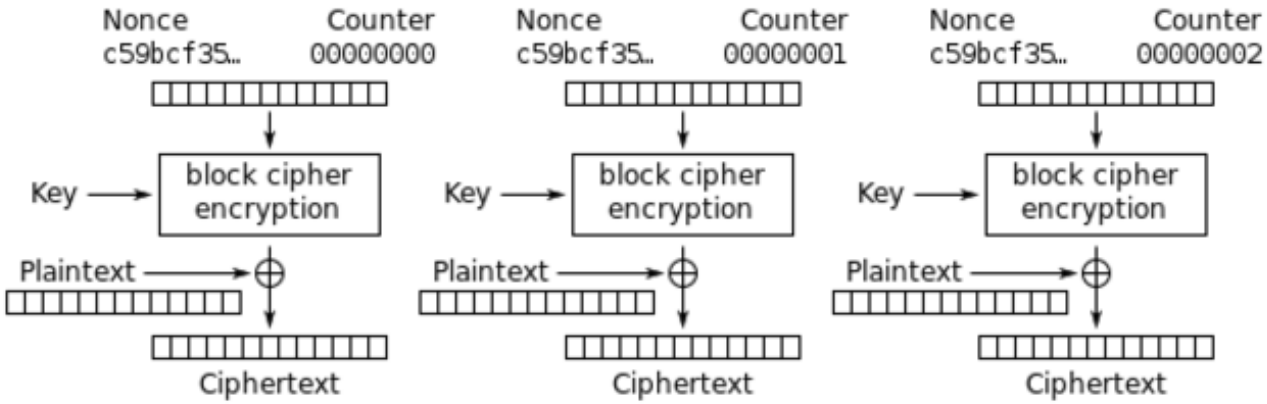
Cipher Block Chaining (CBC) mode decryption

Ataque de substituição no (CBC)

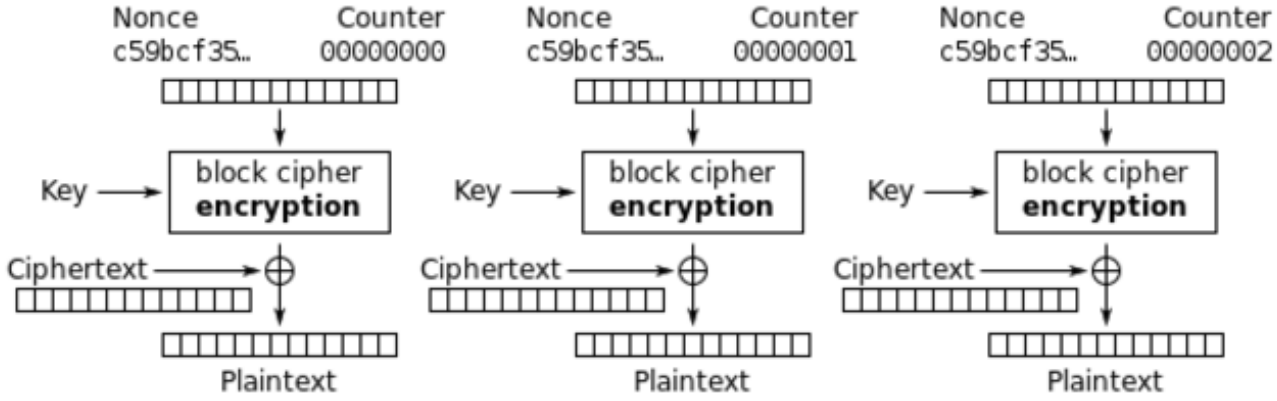
- Suponha o último exemplo (transferência bancária eletrônica).
- Se o IV for escolhido corretamente para cada transferência bancária, o ataque anterior não funcionará.
- Se o IV for mantido para várias transferências, o atacante consegue reconhecer as transferências de sua conta no banco A para o banco B.
- Se escolhermos uma nova IV sempre que encriptamos, o modo CBC torna-se um esquema de criptografia probabilístico, ou seja, duas encritações do mesmo texto claro, são completamente diferentes.
- Não é necessário manter o IV secreto!
- Normalmente, o IV deve ser um valor não secreto. Deve ser usado apenas uma vez!

Counter Mode (CTR)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Counter Mode (CTR)

- Ele usa um cifra de bloco como uma cifra de fluxo.
- O fluxo da chave é calculado em modo bloco.
- A entrada da cifra de bloco é um contador que assume um valor diferente cada vez que a cifra de bloco calcula um novo fluxo de bloco de chave.
- Diferentemente dos modos CFB e OFB, o modo CTR pode ser paralelizado desde que a segunda encriptação pode iniciar antes da primeira ter terminado.
  - É desejável para implementações de alta velocidade, p.e., em roteadores de rede.

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

FIM