Criptografia

Histórico, Técnicas e Aplicações

Tópicos Históricos de Criptografia

Cifras Antigas - Egito

- Tumba de Khnumhotep II
  - Substituição deliberada de alguns símbolos
  - Transformação da escrita com diversos possíveis objetivos
    - Ex.: criar aura de mistério
  - Mais antigo texto conhecido contendo modificação deliberada de linguagem

Cifras Antigas – Esparta – Scytale (Cítala)

- Cifrador espartano de transposição (400AC)
- Fita de papel era enrolada em uma vareta
- Mensagem escrita enquanto a fita está enrolada; depois o papel é removido, ficando a fita com uma seqüência de letras aparentemente aleatória
- A chave é definida pela circunferência da vareta e a espessura do papel

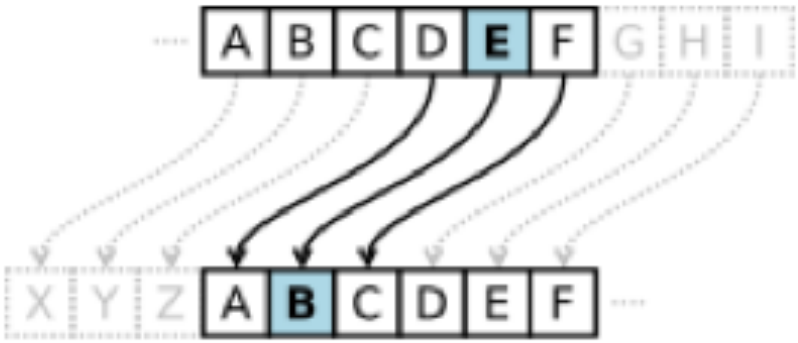
	A	J	U	D	E	
	M	E	S	T	O	
	U	S	O	B	A	
	T	A	Q	U	E	

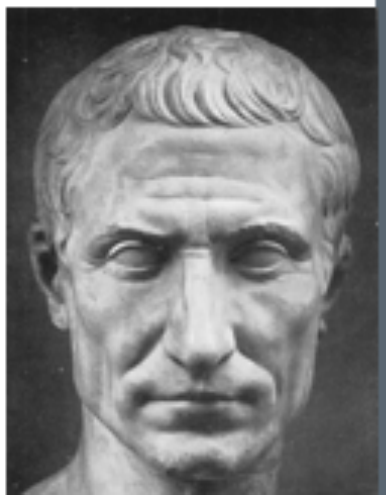
Cifras Antigas – Persas

- Heródoto registra o uso de esteganografia pelos persas (400 AC)
  - Damaratus avisa gregos sobre Xerxes (cera sobre madeira)
  - Histaiaeus envia mensagem a Aristagoras de Miletus (tatuagem no couro cabeludo)

Cifras Antigas – Roma

- Cifras antigas
  - Cifra de substituição supostamente utilizada por Júlio César (100 AC)
  - Basicamente, um "deslocamento" do alfabeto





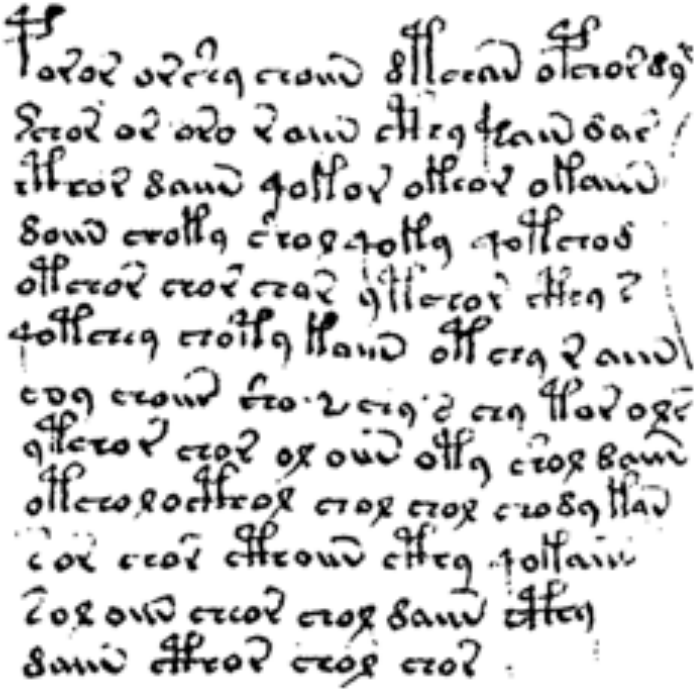
Cifras Antigas – Al-Kindi

- Al-Kindi estuda estatísticas das linguagens e desenvolve primeiras técnicas de criptanálise (séc. IX)
- O "tratado" de criptografia foi redescoberto em 1987, em Istambul
  - Chama-se "Manuscrito sobre 'deciframento' de mensagens criptografadas"

Ahmad al-Qalqashandi

- Ahmad al-Qalqashandi (1355-1418 DC)
- Escreve enciclopédia (Subh al-a 'sha, 14 volumes) com seção dedicada à criptografia (1412 DC)

Manuscrito de Voynich (1450-1520 DC)



Cifra Leon Alberti (1466 DC)

Vigenère

- Livro de Vigenère sobre cifras (1585)
  - Traicte de Chiffres
  - Idéia baseada em Giovan Batista Belaso

Cilindro de Jefferson

Cilindro de Jefferson

- Desenvolvido em 1795
  - 26 discos, cada um com uma ordem aleatória do alfabeto
  - Os discos podem ser reordenados
    - Emissor e receptor "combinam" uma ordenação
  - Emissor gira os discos de maneira a formar a mensagem plana em uma linha
    - Ele transmite a seqüência de caracteres de outra linha
  - Receptor gira os discos de maneira a formar a mensagem cifrada em uma linha
    - A mensagem plana irá aparecer em outra linha

Disco de Wheatstone

- Disco de Wheatstone
  - Originalmente inventado por Wadsworth em 1817
  - Desenvolvido por Wheatstone em 1860
  - Dois discos concêntricos geral uma cifra polialfabética

Urkryptografen: versão do disco de Wheatstone usado pelo exército dinamarquês de 1936 a 1948

Desiderata de Kerchhoff

› Kerchhoff e as leis da criptografia (1883)

JOURNAL

DES

SCIENCES MILITAIRES

DES

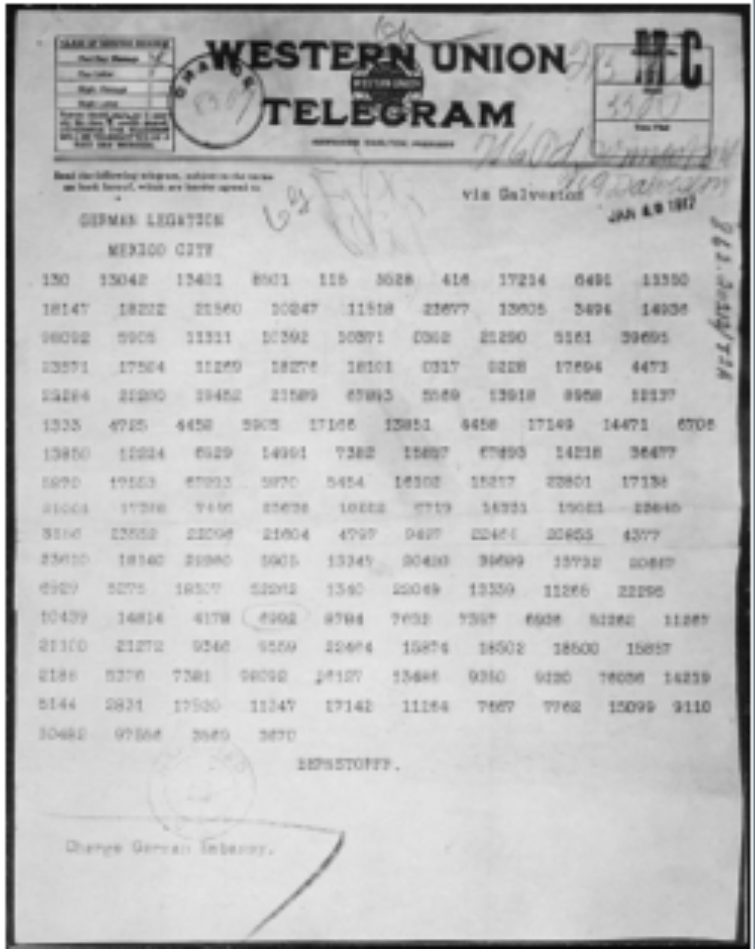
ARMÉES DE TERRE ET DE MER,

PUBLIÉ

SUR LES DOCUMENTS FOURNIS PAR LES OFFICIERS DES ARMÉES FRANÇAISES ET ÉTRANGÈRES,

Telegrama de Zimmerman

› Entrada dos EUA na I Guerra



WESTERN UNION TELEGRAM

via Galveston

GERMAN LEGATION

MEXICO CITY

Enigma

- Importante classe de máquinas cifradoras
- Bastante utilizada durante a Segunda Guerra Mundial
- Discos contendo conexões internas gerando substituições com alfabetos modificados continuamente

Criptografia

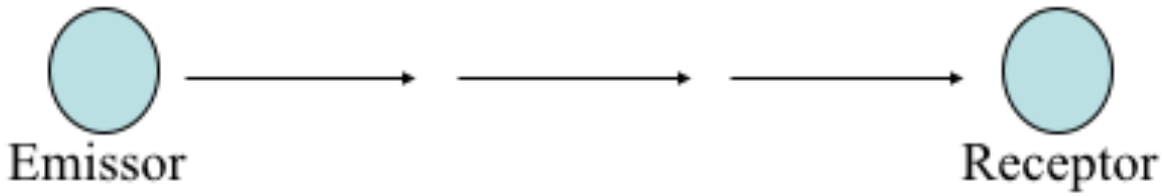
Apresentação

Por que estudar criptografia

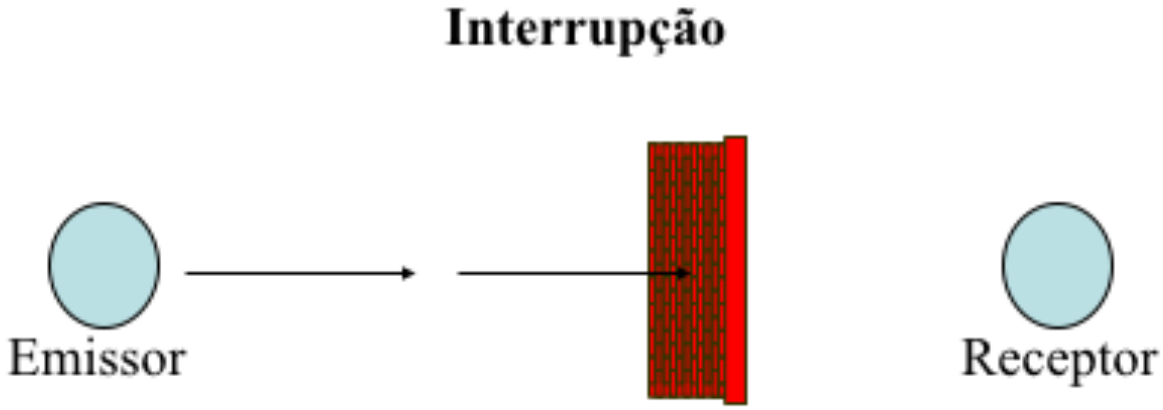
- Ferramenta fundamental para atingir objetivos (prover serviços) de segurança
  - Importante para compreender soluções reais de segurança
- Modelos de funcionamento e de ataques simples e bem-caracterizados
  - Bom ponto de partida para entender arquiteturas de segurança
  - Sempre ter em mente que o mundo real é mais complexo do que os diagramas simplificados que veremos a seguir – lembre dos diversos ataques até agora estudados

Modelo de comunicação "segura"

Fluxo normal da informação



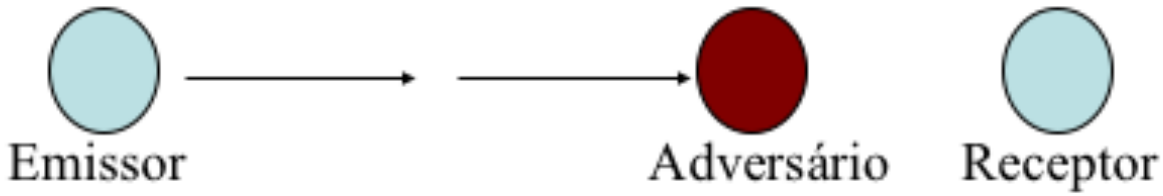
Ataques à segurança: disponibilidade



É um ataque à disponibilidade da informação

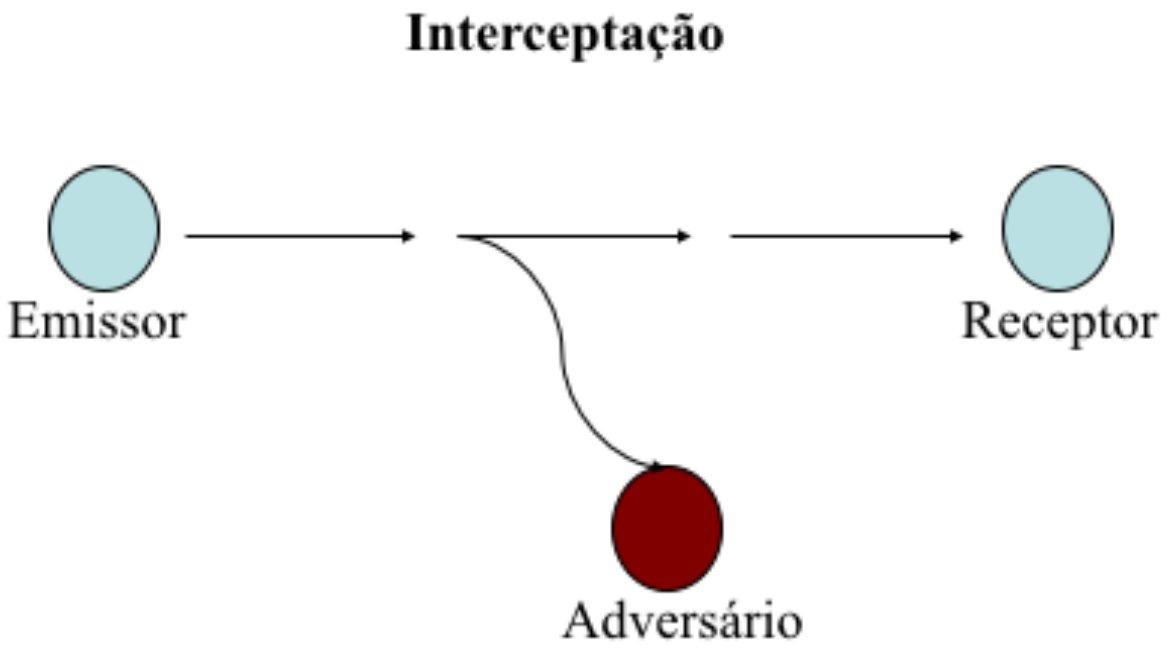
Ataques à segurança: disponibilidade

Interrupção



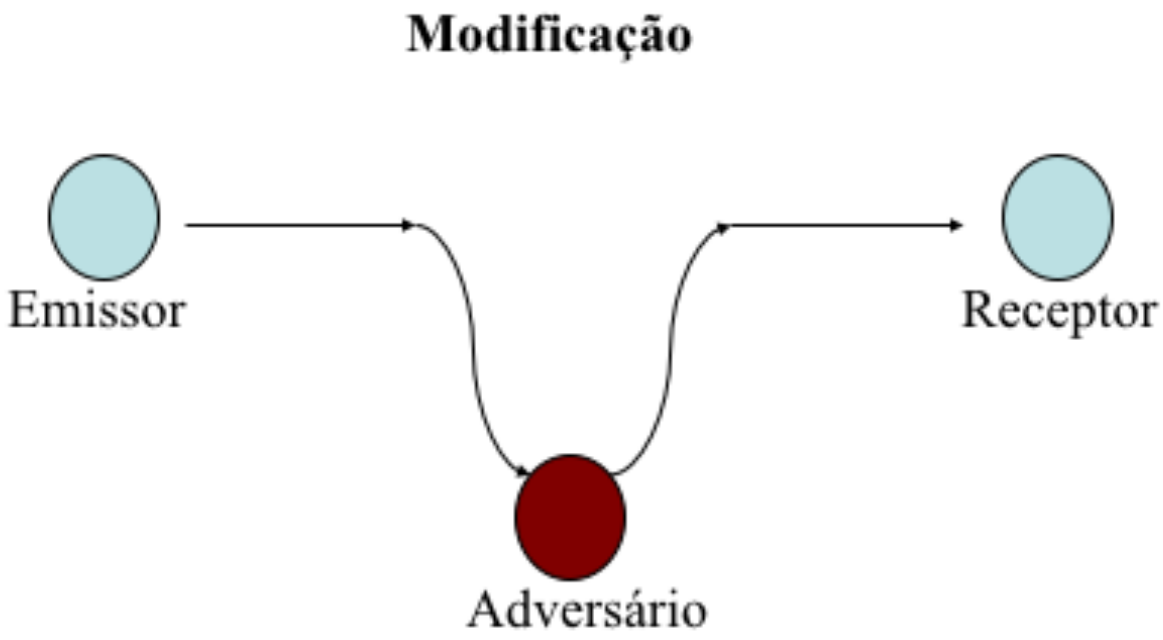
É um ataque à disponibilidade da informação

Ataques à segurança: confidencialidade



É um ataque à confidencialidade da informação

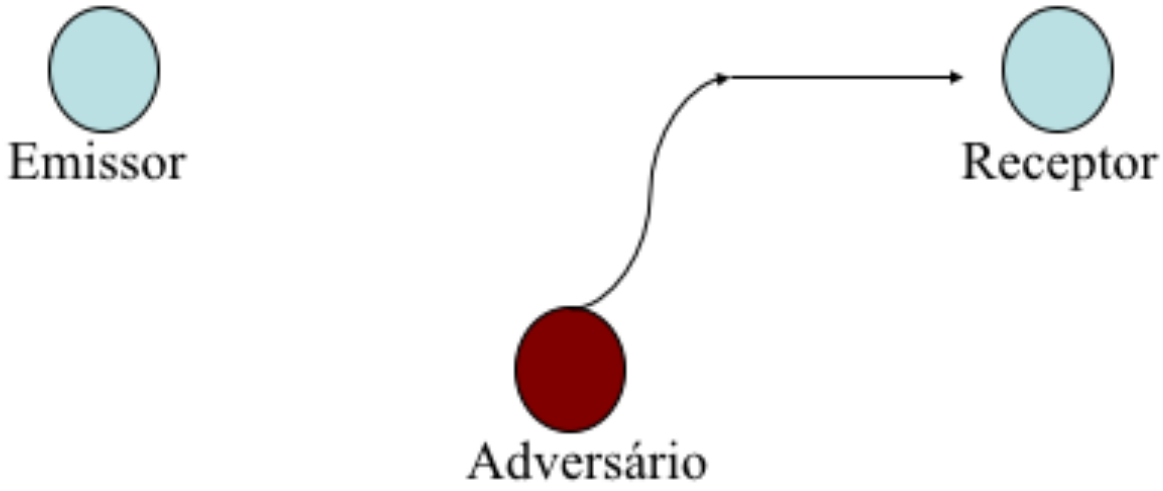
Ataques à segurança: integridade



É um ataque à integridade da informação

Ataques à segurança: autenticidade

Fabricação



É um ataque à autenticidade da informação

O que é criptografia?

- Uma ferramenta matemática para atingir objetivos de segurança da informação
  - De fato, é elemento fundamental, presente na maioria das soluções de segurança
  - Frequentemente não será a única ferramenta
  - Outras ferramentas:
    - Assinatura (clássica X digital)
    - Lacres
    - Lei (exemplo da violação de correspondência)
    - Políticas de segurança
    - Controle do acesso físico

Criptografia

- **escrita** (-grafia) **secreta** (cripto-)
- Terminologia
  - Texto plano ou mensagem plana – mensagem original
  - Texto cifrado ou mensagem cifrada – mensagem codificada
  - Transformação criptográfica – função que leva textos planos a cifrados (trans. de encriptação) ou textos cifrados a planos (transf. de decriptação)
  - Chave - informação que determina uma transformação criptográfica a ser utilizada

Criptografia

- Terminologia
  - Criptografar (encriptar) – converter texto plano em cifrado
  - Cifra – conjunto de transformações criptográficas indexadas por chaves
  - Descriptografar (decriptar) – converter texto cifrado em plano

Criptografia

- Terminologia
  - criptografia – estudo dos princípios e métodos de encriptação
  - criptanálise – estudo dos princípios e métodos para descriptografar sem o conhecimento da chave
  - criptologia – campo de estudo da criptografia e criptanálise
  - código – algoritmo que transforma uma mensagem compreensível em uma incompreensível a partir de um livro de códigos (ex.: códigos militares)

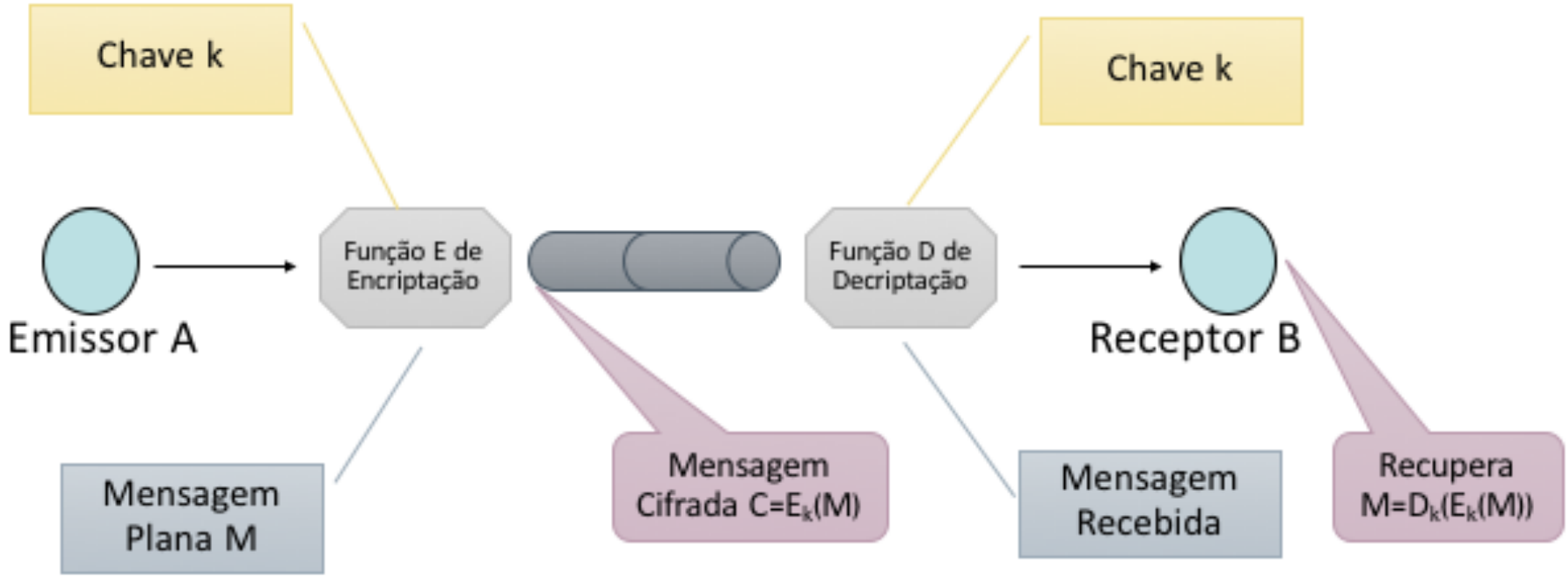
Ferramentas criptográficas Básicas

- Cifras (chave simétrica, bloco)
  - Objetivo: "confidencialidade" da informação
  - Chave "simétrica": mesma chave para encriptar e decriptar
- Hash (Resumo Criptográfico)
  - Objetivo: integridade da informaçao
  - Não usa chaves
- Códigos de Autenticação de Mensagem (MAC)
  - Objetivo: autenticação de origem da informação
  - Chave "simétrica": mesma chave para autenticar e verificar
- Acordo de Chaves Diffie-Hellman
  - Estabelecimento de chaves sem transmissão pelo canal
- Cifras (chave assimétrica)
  - Cifra com chaves distintas para encriptar e decriptar
  - Cada usuário possui uma chave privada e uma chave pública
- Assinatura Digital
  - Ferramenta para autenticidade e irrefutabilidade
  - Cada usuário possui uma chave privada e uma chave pública
- Cifras de Stream
  - Encripta no nível do bit
  - Modelo de chave simétrica
- Geradores de Números Aleatórios
  - Números aleatórios são usados extensivamente em criptografia
- Gerenciamento de chaves
  - Estabelecimento de Chaves
  - Certificação Digital (PKI)

Cifras (chave simétrica, em bloco)

- Aplicação clássica da criptografia
  - Objetivo: proteger mensagens em trânsito
- Tradicionalmente, assumia sigilo do algoritmo
  - Conceito moderno: apenas a chave fica secreta
- Cifra em bloco: opera sobre blocos de bits
  - Em oposição a cifras de fluxo, que operam bit-a-bit

Modelo para cifra simétrica



Cifras Clássicas

Cifra de César (Substituição)

- k=3
- Msg Plana:

VIM VI VENCI

- Mensagem cifrada

YLP YL YHQFL

Cifra de Cítala (Transposição)

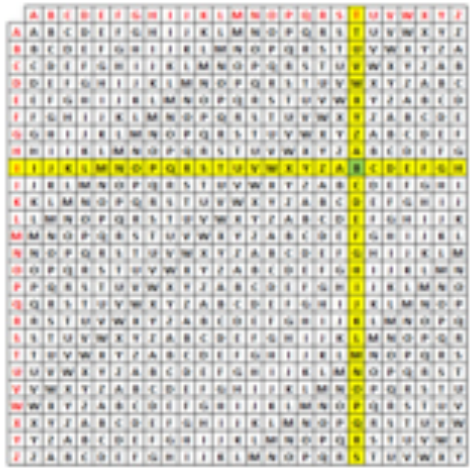
- k=2
- Msg Plana: ENCONTRE FRONT

E C N R F O T
N O T E R N

- Mensagem cifrada

E C N R F O T N O T E R N

Cifra de Gronsfeld-Vigenàre (Mistura com Chave)



- k=GREEN
- Msg Plana:

HELLO HOW ARE YOU

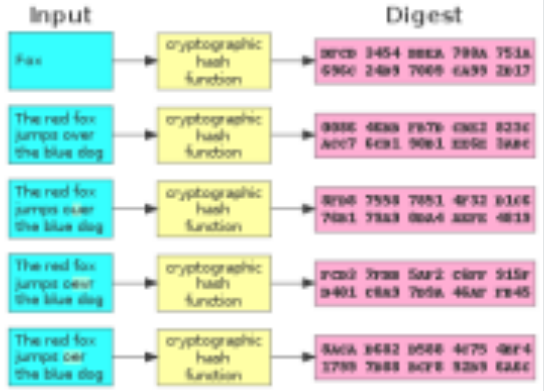
- Mensagem cifrada

NVPPB NFA EEK PSY

Modelos de Ataque

- Ataques criptanalíticos versus ataques a protocolos
- Exemplo de ataque a protocolo: transferência bancária
  - Mensagem de transferência contendo vários campos criptografados separadamente
- Tipos de ataques criptanalíticos
  - Ciphertext-only
  - Known-plaintext
  - Chosen (plain/cipher)text

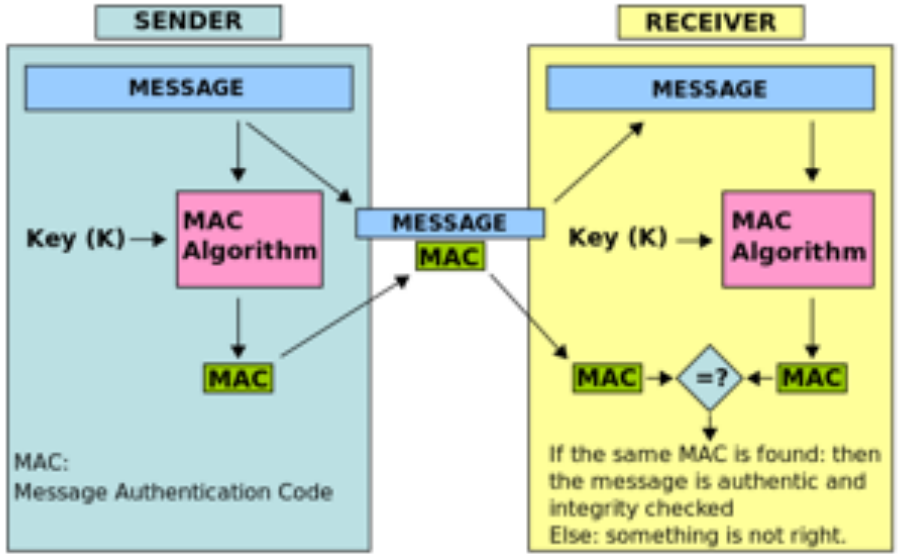
Hash (Resumo Criptográfico)



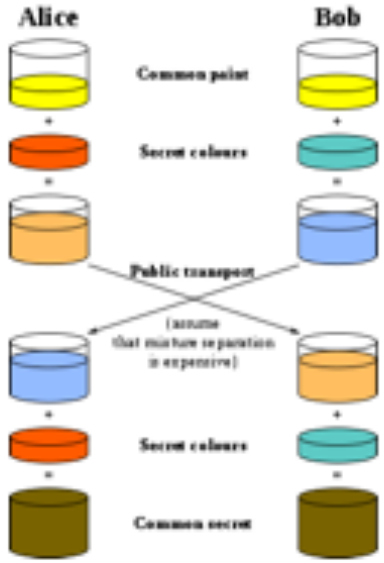
- Função criptográfica sem chave
  - Entrada: mensagem de tamanho "arbitrário"
  - Saída: mensagem de tamanho fixo (centenas de bits)
- Funciona como identificador "seguro" da mensagem
- Baseia-se nas propriedades de resistência a colisão:
  - Resistência a ataque de pré-imagem (one-way)
  - Resistência fraca a colisão (segunda pré-imagem)
  - Resistência forte a colisão
- Hashes ingênuos (não-cripto): truncar, cifrar XOR de blocos
- Hashes modernos construídos com operações de substituição, permutação etc.
- Aplicações: versão de software, imagem de disco em forense, controle de acesso em Unix

Códigos de Autenticação de Mensagem (MAC)

- Espécie de resumo criptográfico dependente de chave
  - Resumo associado à mensagem, chave autentica origem
- Enviado junto à mensagem, identificando origem
- Resistência a colisões e inversões (assim como hash)



Acordo de Chaves Diffie-Hellman

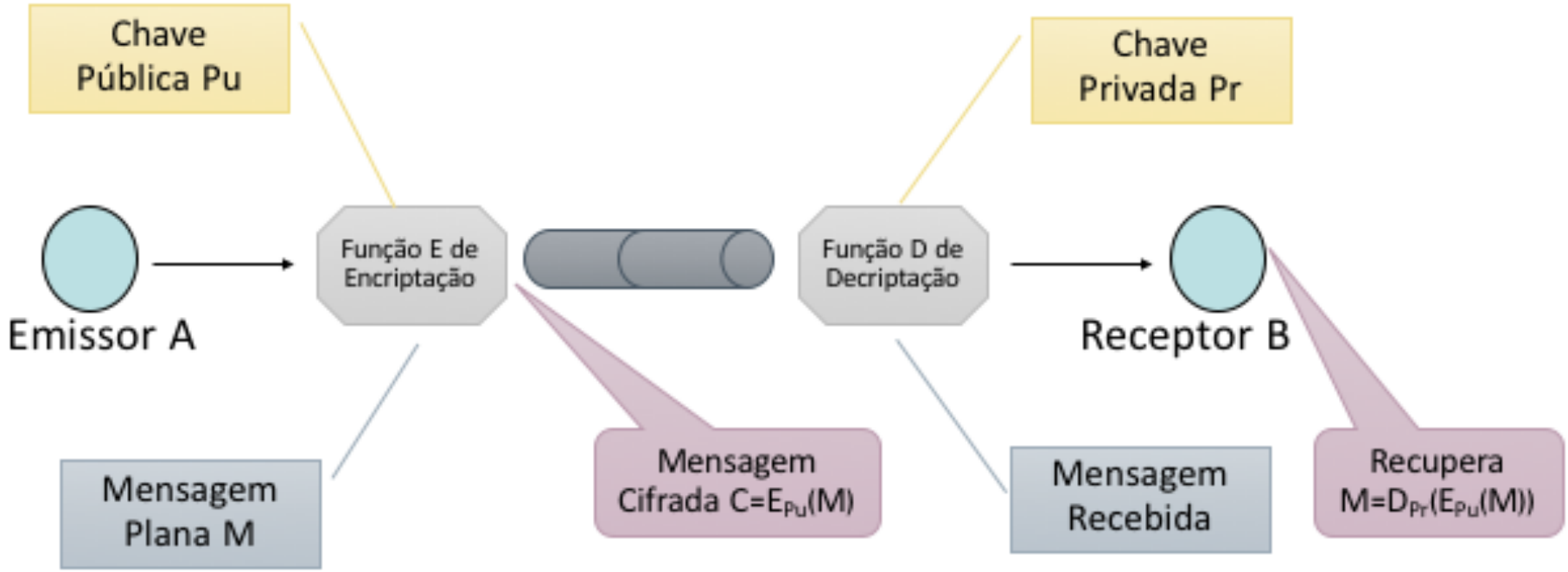


- Permite que duas partes concordem remotamente sobre uma chave criptográfica
- Chave criptográfica é construída a partir de informações trafegadas na rede
  - Alice sorteia k_A e envia $f(k_A)$
  - Bob sorteia k_B e envia $f(k_B)$
  - Alice constrói $g(k_A,f(k_B))$ igual a $g(k_B,f(k_A))$ construído por Bob
- Alice e Bob passam a usar $k=g(k_A,f(k_B))=g(k_B,f(k_A))$
- Não é possivel recuperar k a partir das informações trafegadas $f(k_A)$ e $f(k_B)$

Cifras de chave pública (chave assimétrica)

- Ferramenta de confidencialidade
- Assimetria entre encriptação e decriptação
  - Uma chave (pública) encripta e outra (privada) decripta
- Maior quebra de paradigma da história da criptografia
  - Primeiro algoritmo prático desenvolvido por Rivest, Shamir e Adleman em 1976
  - Algoritmo era conhecido pela inteligência britânica desde 1973 (Cocks)
- Baseia-se na "dificuldade computacional"
  - Assimetria na complexidade de computar f e f^{-1}
  - Exemplos: multiplicação de primos, exponenciação discreta

Modelo para cifra assimétrica



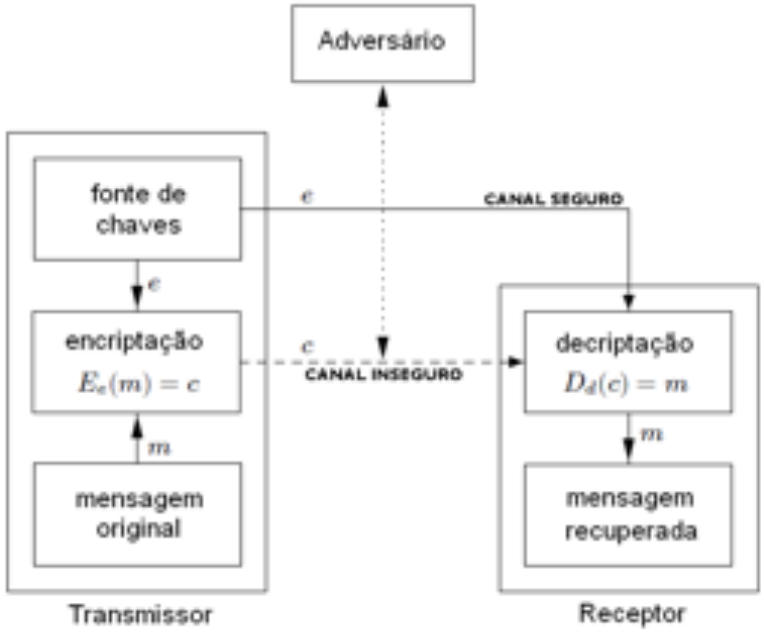
Analogias: chave simétrica vs chave pública

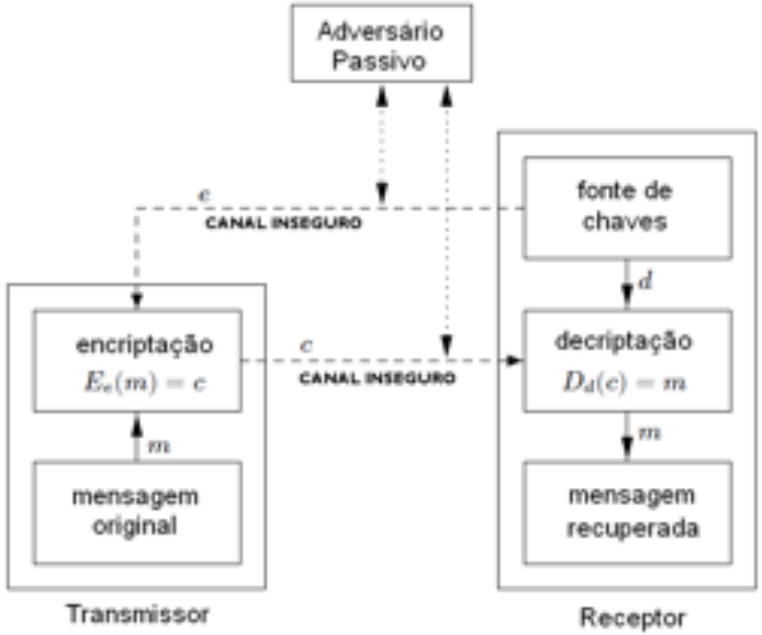
- Chave simétrica: cadeados e chaves
  - Conjunto de pessoas possui chave de cadeado de caixa
  - Apenas essas pessoas podem inserir algo na caixa e trancar
    - Equivalente a encriptar mensagem
  - Exatamente essas pessoas podem retirar da caixa trancada
    - Equivalente a decriptar mensagem
- Chave pública: cadeados e chaves
  - Cada pessoa possui um cadeado e sua respectiva chave
  - Cada pessoa pode disponibilizar cadeados abertos
    - Ou seja, divulgar sua chave pública
  - Qualquer um pode trancar uma caixa com o cadeado
    - Ou seja, encriptar mensagens
  - Apenas o dono da chave pode abrir o cadeado (e a caixa)
    - Ou seja, decriptar mensagens

Analogias: chave simétrica vs chave pública

- Chave simétrica: cofre
  - Conjunto de pessoas possui segredo do cofre
  - Apenas essas pessoas podem inserir algo
    - Equivalente a encriptar mensagem
  - Exatamente essas pessoas podem retirar algo
    - Equivalente a decriptar mensagem
- Chave pública: caixa de correio
  - Cada pessoa possui uma caixa
  - Qualquer pessoa pode inserir mensagem
    - Ou seja, encriptar a mensagem
  - Apenas o dono da caixa pode retirar as mensagens
    - Ou seja, decriptar as mensagens

Comparando os modelos

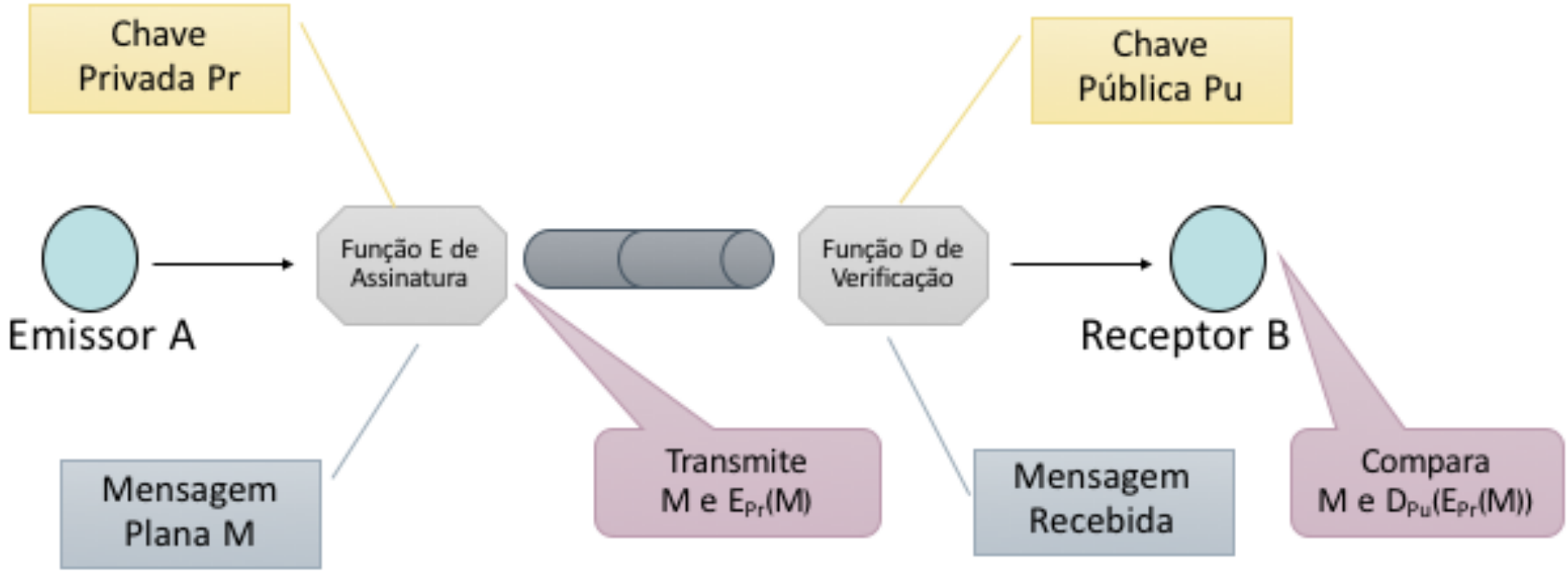




Assinatura Digital

- Um tipo de criptografia assimétrica
  - Inversa da cifra de chave pública
- Espécie de resumo criptográfico da mensagem construído a partir da chave privada
  - Assim, provê não-repúdio
- Mensagem enviada acompanhada da assinatura digital
  - Não provê confidencialidade

Modelo para assinatura digital



Cifras de Stream

- Cifras de stream criptografam bit a bit – em oposição à cifra de bloco
- Exemplo da Cifra de Vernam – one-time pad
  - Única cifra com segurança incondicional
  - Desvantagem do tamanho da chave
- Cifras de stream práticas: keystream gerada a partir uma semente compartilhada entre as partes

Geradores de Números Aleatórios

- Conceito de "aleatoriedade"
- True Random Number Generator (TRNG)
  - Números aleatórios a partir de eventos físicos
- Pseudo Random Number Generator (PRNG)
  - Números "aparentemente" aleatórios gerados por algoritmos determinísticos – possibilita reprodutibilidade
- Estrutura típica
  - TRNG como fonte de entropia que é inserida em um PRNG
- Aplicações
  - Criação de chaves criptográficas
  - Cifras de stream (fluxo de bits a serem XORed com mensagem)
  - Criação de nounces/IV em protocolos e modos de operação
  - Desafios em protocolos challenge-response
  - Aplicações em protocolos diversos (de sorteio a assin. contratos)

Gerenciamento de Chaves

- Estabelecimento de chaves: acordo versus transporte
- Problema prático: como as partes podem concordar a respeito de chaves criptográficas?
  - Difícil resolver se não temos um canal autenticado
- Modelo "mais seguro": as partes se encontram pessoalmente e definem suas chaves
  - Não é prático se temos redes globais envolvendo bilhões de pessoas e dispositivos
- Certificado digital: associação entre identidade e chave pública certificada por TTP
- PKI: estrutura hierárquica de TTPs para certificação digital
  - Alguns TTPs emitem certificados de chave pública
  - Outros TTPs autorizam a "operação" de TTPs na rede
  - Um TTP é a "raiz" da estrutura e origem da confiança

Criptografia

Visão do Livro =)

Funções unidirecionais e hash criptográfico

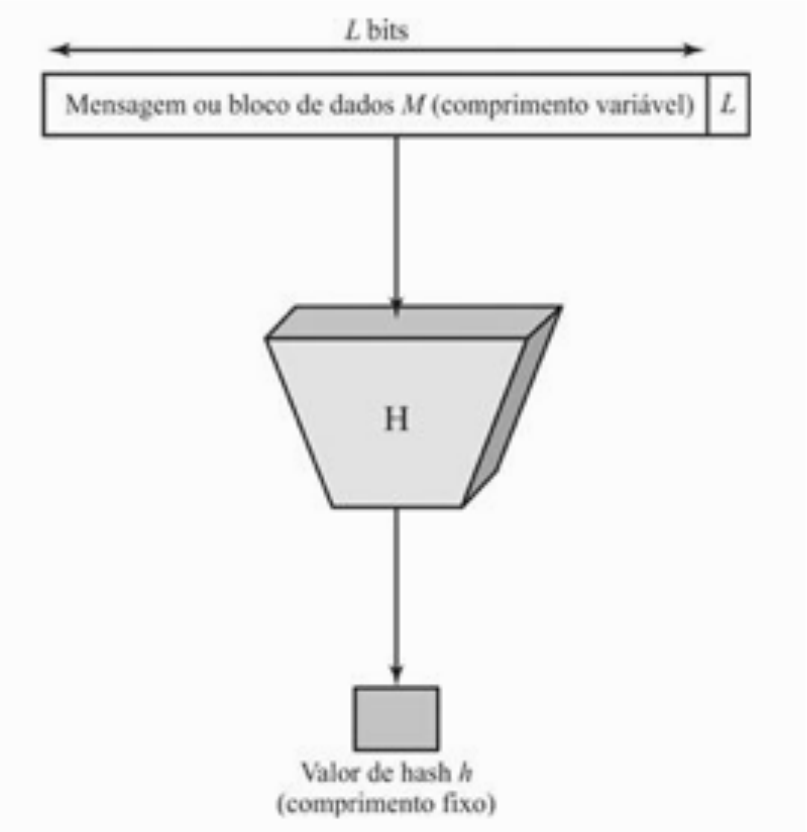
- Função unidirecional: fácil computar, difícil inverter
  - "A" ferramenta fundamental da criptografia
  - Exemplo: $f(x)=3^x \bmod 17$
- Hash criptográfico: recebe como entrada uma mensagem e gera um pequeno "resumo"
  - É uma função unidirecional: inviável encontrar mensagem a partir de um resumo
  - Resistência a colisões: inviável encontrar duas mensagens com o mesmo resumo
  - Não confundir com tabela de dispersão e hash não-criptográfico

Exemplo de função unidirecional

- Seja $X=\{1,\ldots,16\}$ e $f(x)$ o resto da divisão de 3^x por 17
  - Dado $x \in X$, é relativamente fácil obter $f(x)$
  - Entretanto, não é tão fácil obter, por exemplo, o valor de x tal que $f(x)=7$.
    - Provavelmente teremos que tentar todas as 16 possibilidades

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Lógica do hash criptográfico

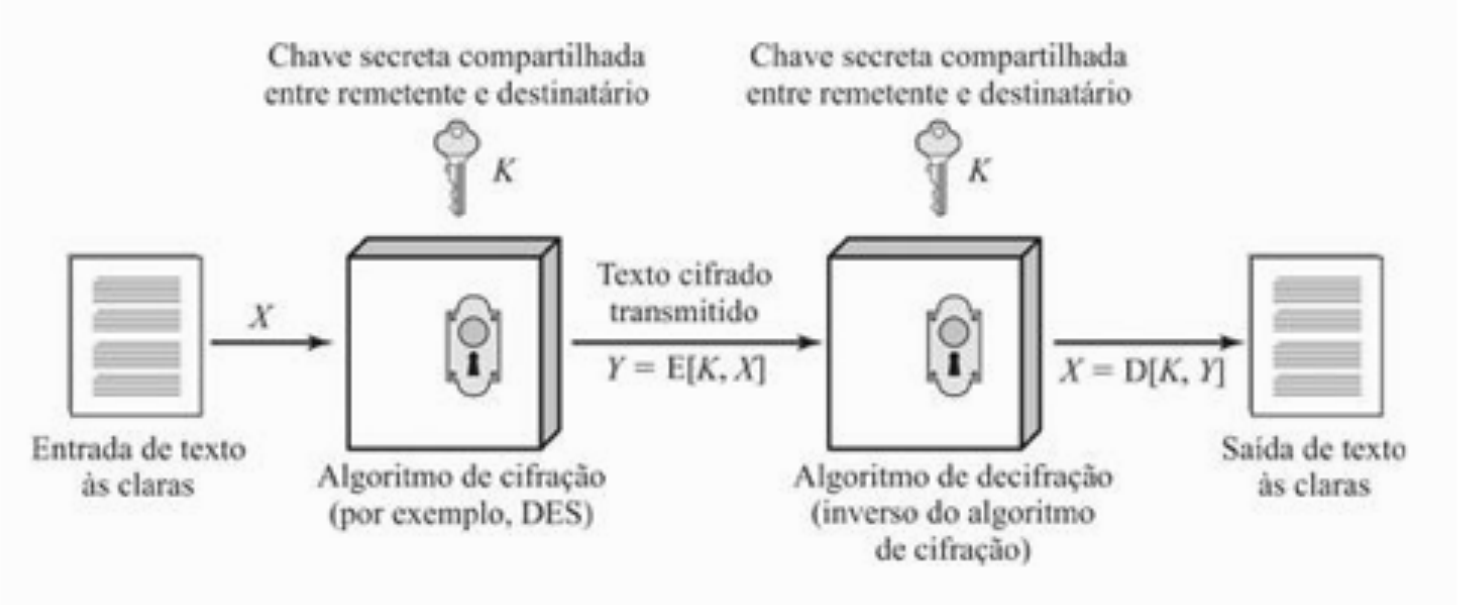


Segurança da função hash

- Resistência a identificação de pré-imagem
  - Para qualquer código dado h, é inviável em termos computacionais achar x tal que H(x) = h.
- Resistência fraca a colisão
  - Para qualquer mensagem dada x, é inviável em termos computacionais achar y ≠ x tal que H(y) = H(x).
- Resistência forte a colisão
  - É inviável, em termos computacionais, achar qualquer par (x, y) tal que H(x) = H(y).

Cifração Simétrica

- Texto em claro / às claras
- Algoritmo de cifração
- Chave secreta
- Texto cifrado
- Algoritmo de decifração



Algoritmo de cifração de bloco

- Cifra mensagem processando-a em ”blocos” de tamanho fixo.
- Algoritmos mais importantes
  - Data Encryption Standard (FIPS PUB 46)
  - Triple DES (ANSI X9.17 e FIPS PUB 46-3)
  - Advanced Encryption Standard (FIPS PUB 197)
- Modos de operação – como trabalhar com blocos em mensagens longas
  - Exemplo mais simples: ECB

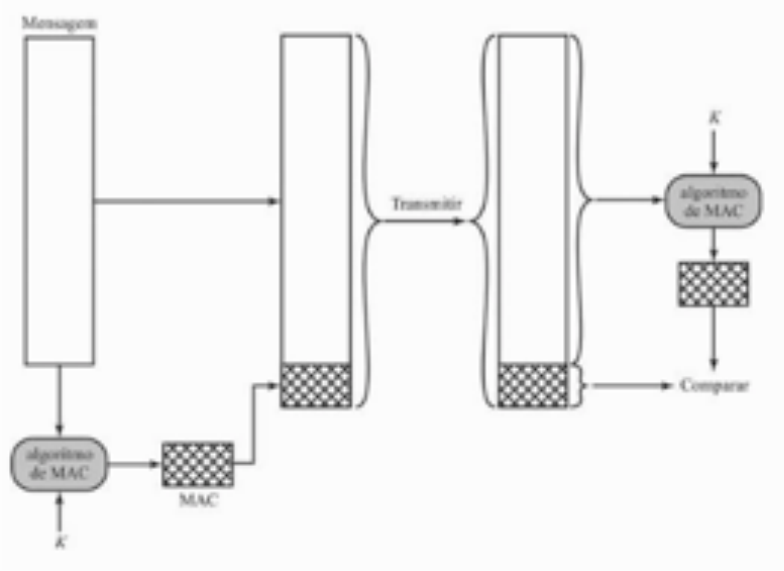
Cifra de fluxo

- Processa mensagem bit-a-bit (ou byte-a-byte)
- Estreitamente relacionada a geradores de números aleatórios
  - Exemplo de abordagem: XOR entre os bits da mensagem e os bits de um PRNG

Autenticação de mensagem e funções hash

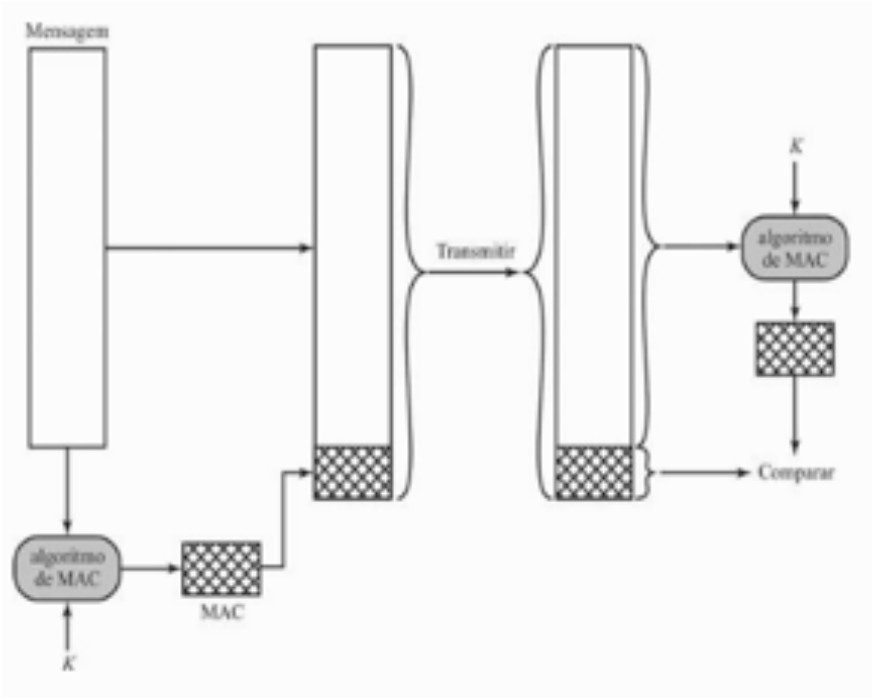
› Autenticação com cifra simétrica
  – Mensagens válidas devem compor um código

› Autenticação sem cifra simétrica
  – Mensagem segue junto com código de autenticação

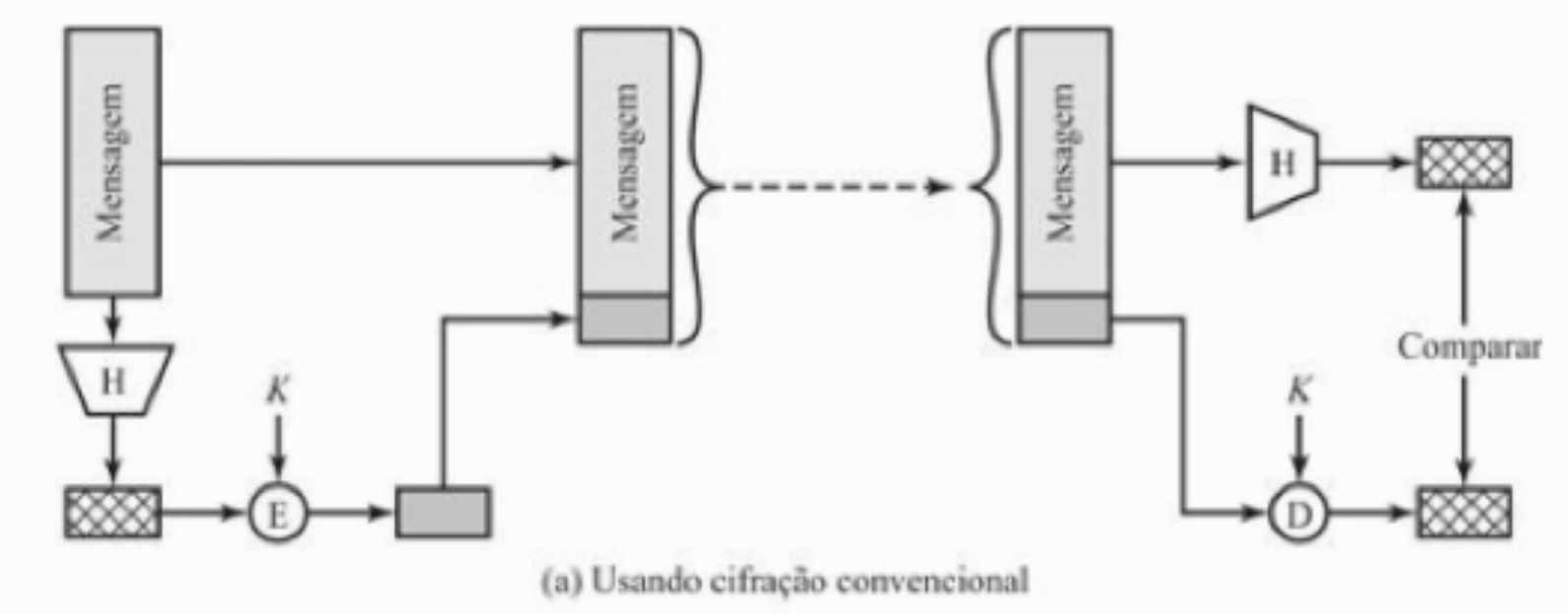


Message authentication code (MAC)

- Recebe como entrada uma mensagem M e uma chave secreta K_{AB} e gera como saída um pequeno bloco de dados $MAC_M=F(K_{AB},M)$, o cód. aut. mensagem
- Trasmissor envia M e MAC_M
- Receptor recalcula $F(K_{AB},M)$ e compara com MAC_M recebido
- Funciona porque só se pode gerar MAC_M conhecendo-se a chave secreta K_{AB}

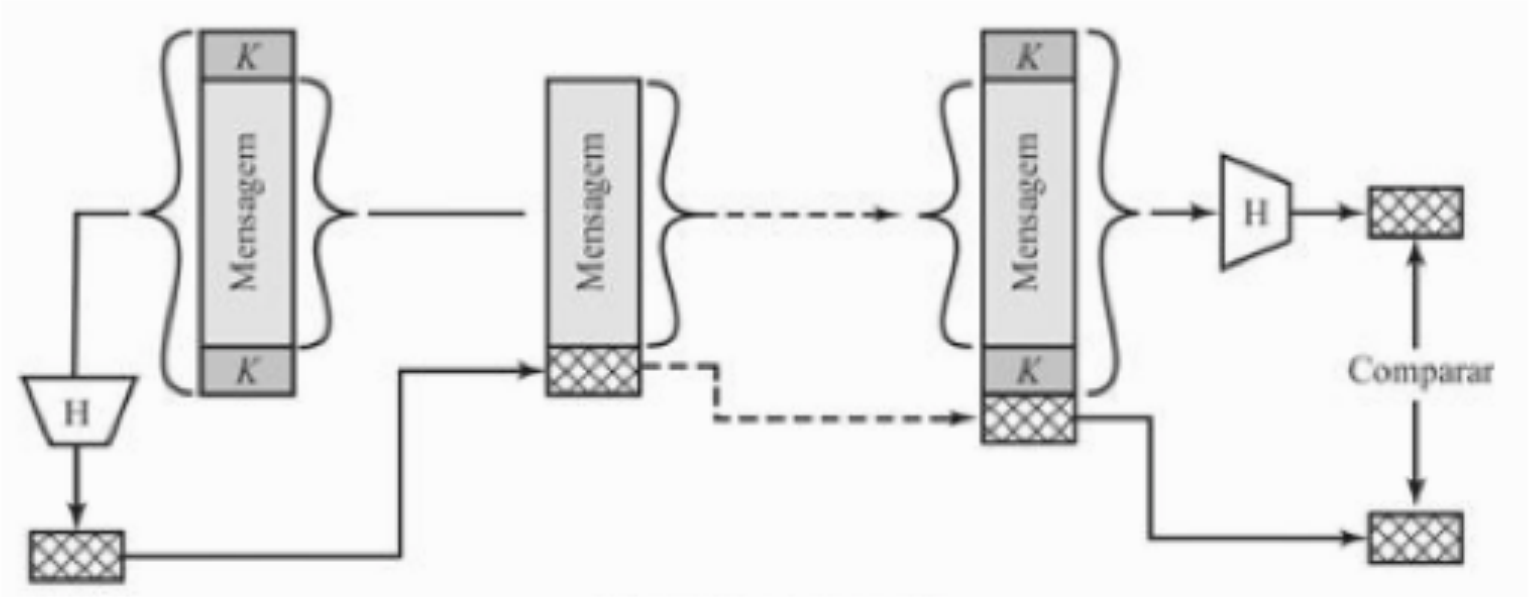


Autenticação com cifra simétrica

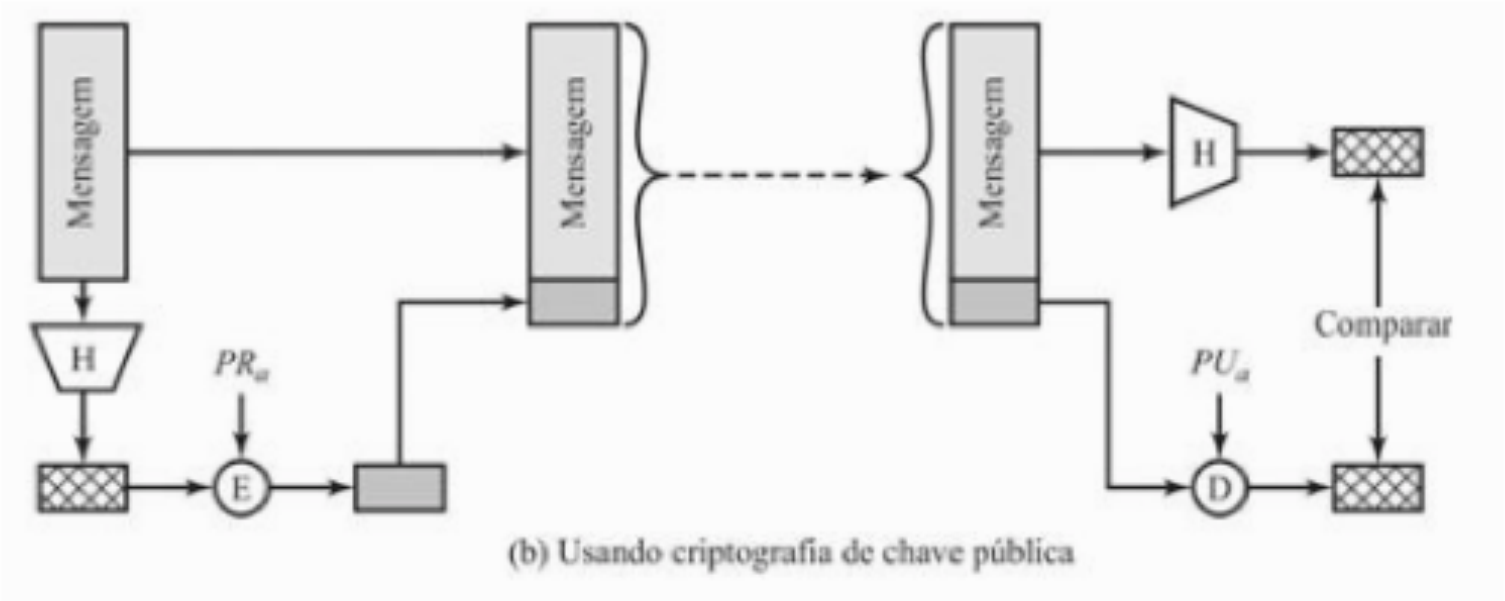


(a) Usando cifração convencional

Autenticação com hash/MAC



Autenticação com chave pública



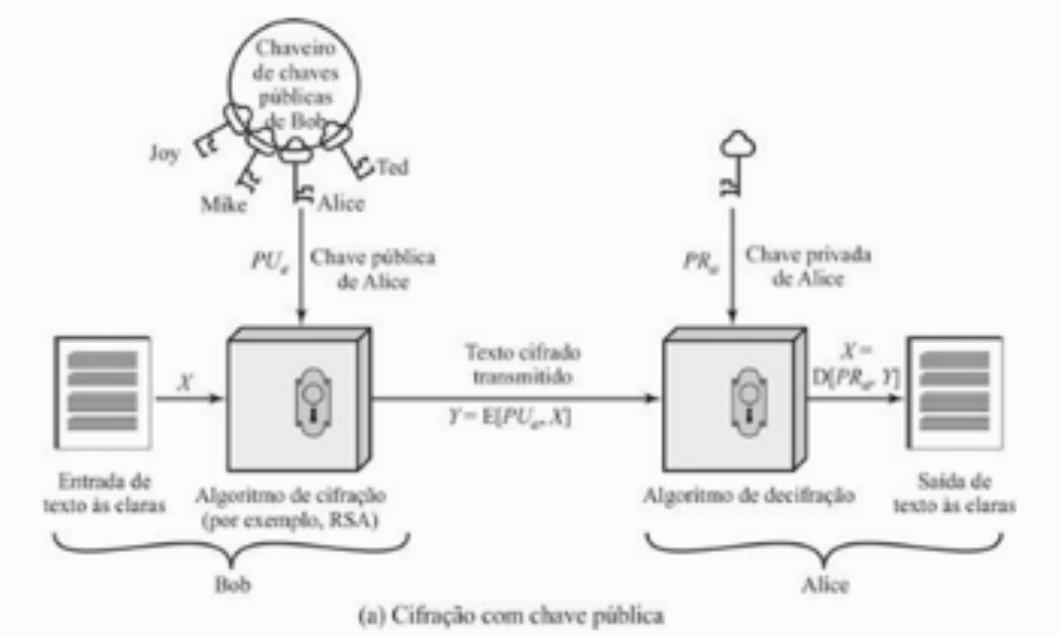
(b) Usando criptografia de chave pública

Criptografia de chave pública

› Acordo de chaves: Diffie e Hellman, 1976

› Cifra de chave pública: Rivest Shamir e Adleman, 1977

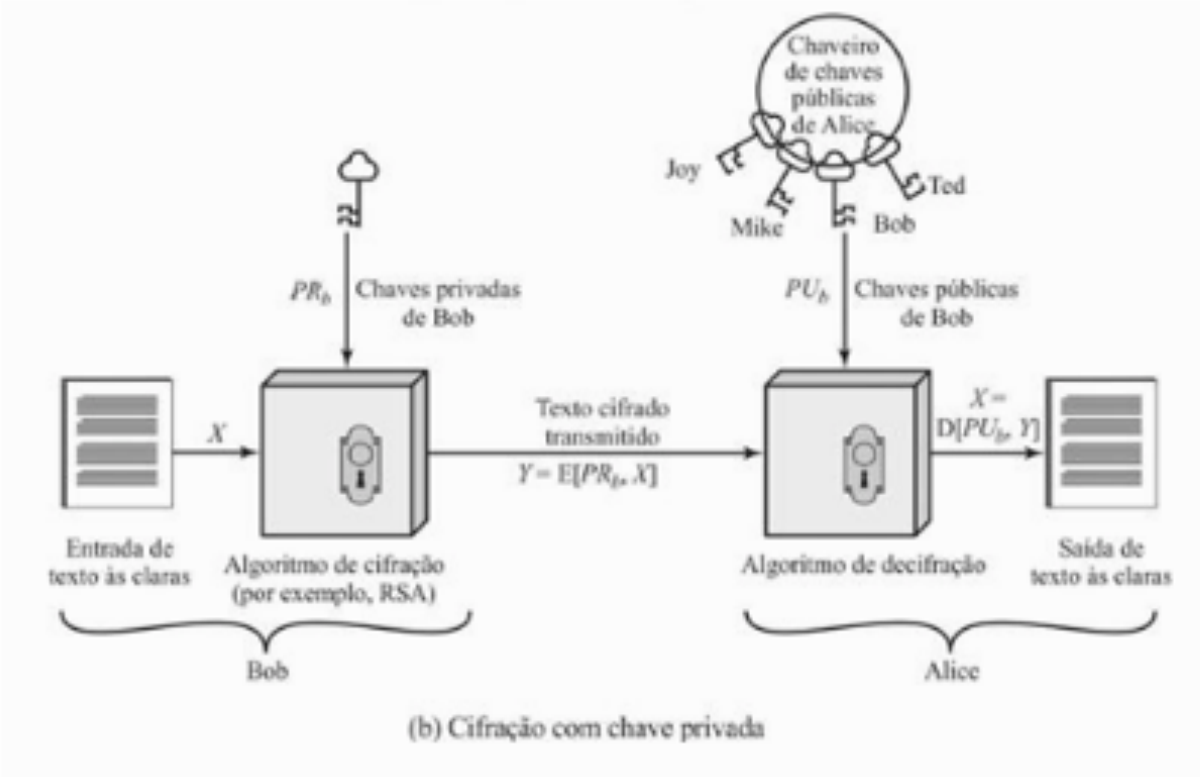
› Supostamente conhecido pelo GCHQ em 1973



(a) Cifração com chave pública

Assinaturas digitais

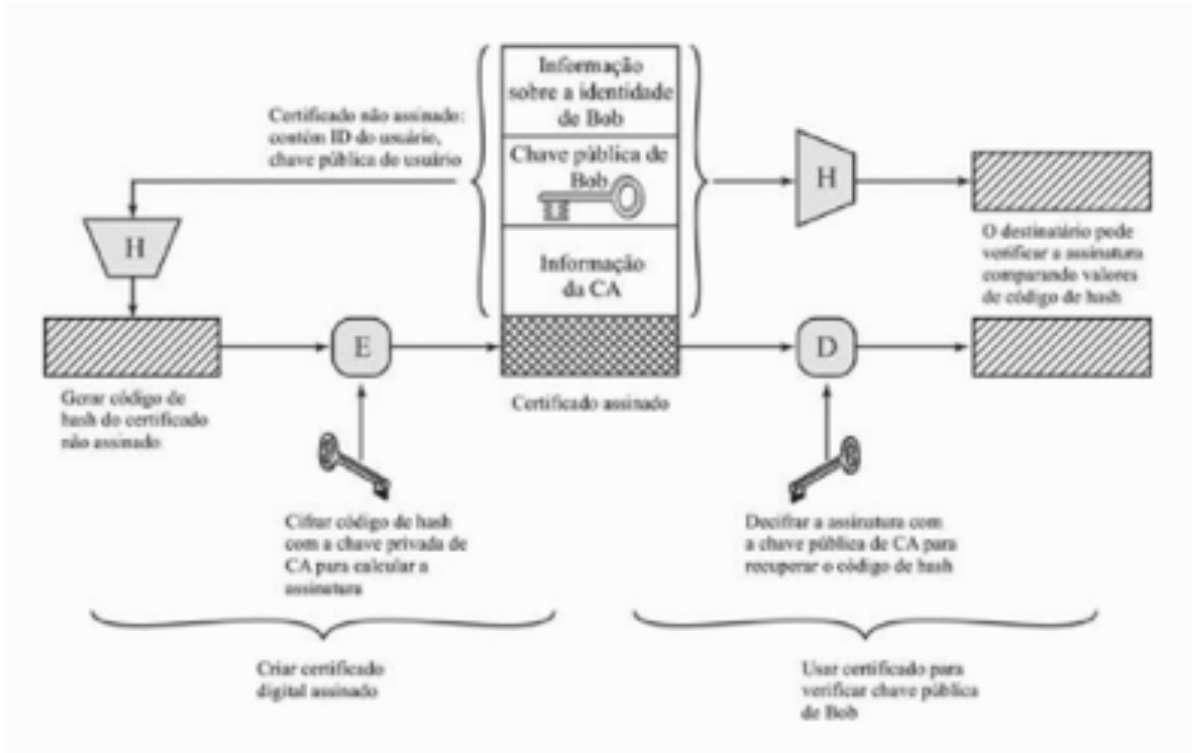
› Uso da chave privada para atestar a origem



(b) Cifração com chave privada

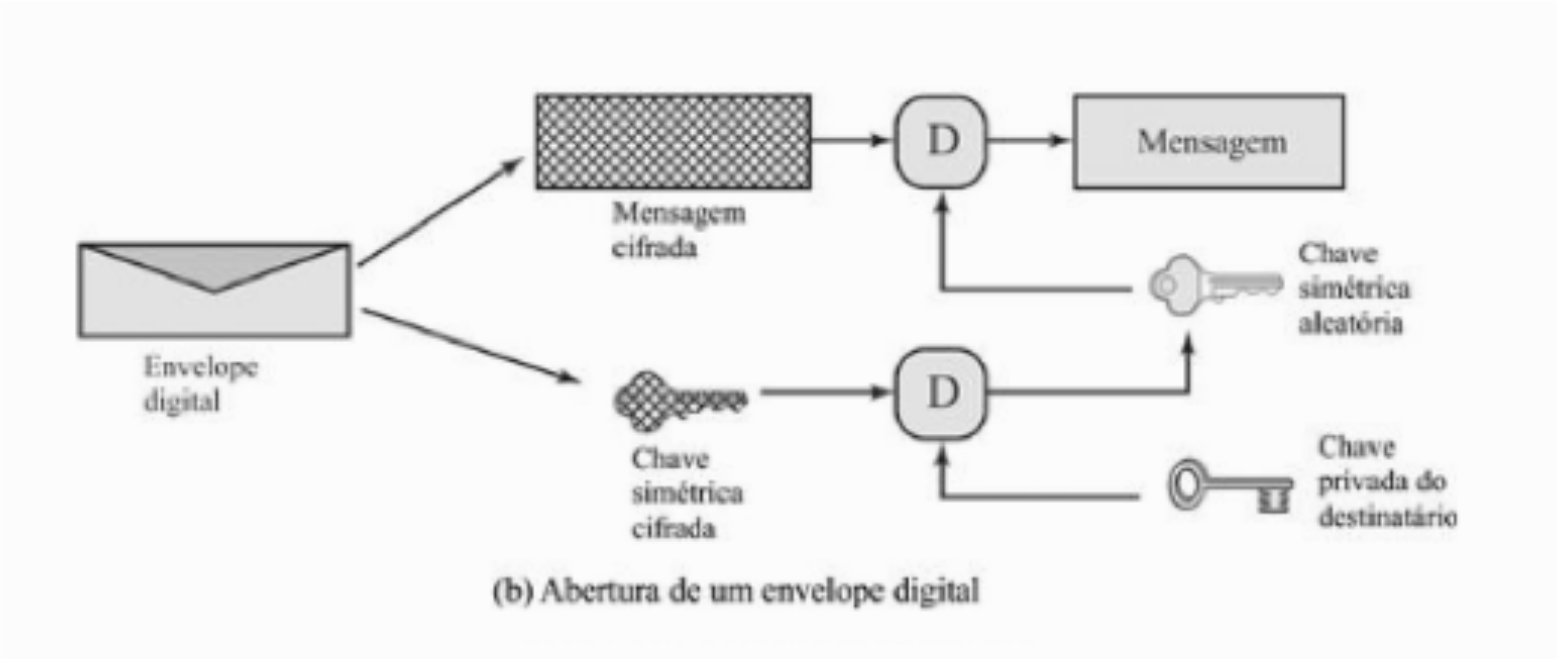
Certificados de chave pública

› Associação entre "identidade" e "chave pública" realizada por terceiras partes confiáveis



Envelope digital

› Mensagem é cifrada simetricamente e a chave é cifrada com a chave pública do destinatário



(b) Abertura de um envelope digital

Cifras modernas de bloco com chave simétrica

Cifras de bloco

- Cifras de bloco quebram a mensagem e a encriptam bloco a bloco
- É como uma substituição de caracteres “longos” (64-bits ou mais)
- A maioria das cifras mais populares na atualidade são deste tipo

Princípios das cifras de bloco

- Cifras de bloco funcionam como uma grande substituição
  - Para blocos de 64 bits, cada uma das 2^{64} mensagens planas é levada, de forma bijetiva, em uma de 2^{64} mensagens cifradas
- Construir tal tabelas de substituições seria impraticável
- Muitos dos cifradores de bloco modernos são baseados na chamada Estrutura de Cifra de Feistel
- Utilizam-se blocos menores de construção
- Então, usa-se a idéia de composição de cifras

Cifras de bloco iteradas

- Envolve a repetição de funções internas chamadas rounds
- São parâmetros da cifra
  - Número de rounds
  - O tamanho do bloco
  - O tamanho da chave, de onde serão tiradas as subchaves de cada round
- Cada round deve ser uma função bijetiva

Estrutura das cifras de Feistel

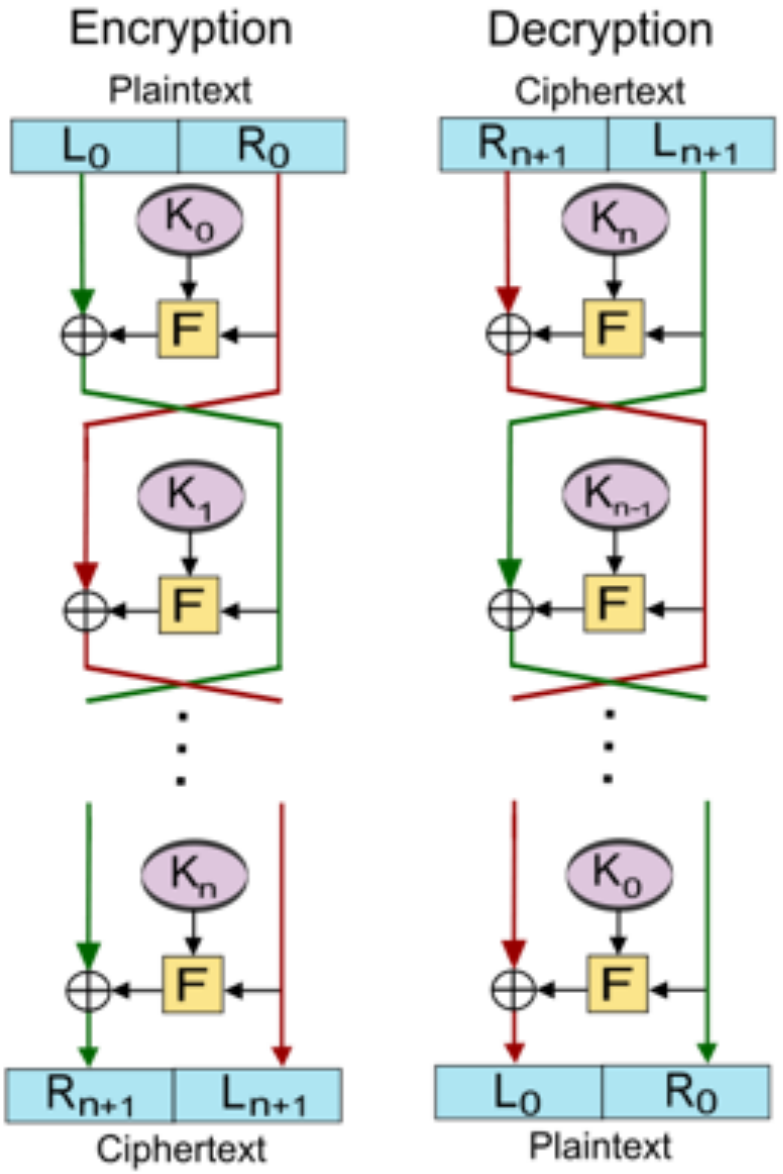
- Desenvolvida por Horst Feistel
- Particiona o bloco de entrada em duas partes de mesmo tamanho
- Processa em rounds nos quais
  - Aplica substituição, na metade esquerda, baseada no conteúdo da metade direita e em subchave derivada da chave
  - Então, permuta as duas partes
- Formalmente:
  - $L_i = R_{i-1},\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Decriptação da Cifra de Feistel

- Tipicamente, $r \geq 3$ rounds
- Ordena a saída como (R_r, L_r)
- Decriptação: apenas aplicar os rounds na ordem reversa

Estrutura da cifra de Feistel

- Cifras de Feistel ou modificações da cifra de Feistel: Blowfish, Camellia, CAST-128, DES, FEAL, ICE, KASUMI, LOKI97, Lucifer, MARS, MAGENTA, MISTY1, RC5, TEA, Triple DES,Twofish, XTEA, GOST 28147-89
- Generalizações da cifra de Feistel: CAST-256, MacGuffin, RC2, RC6, Skipjack, SMS4, CLEFIA



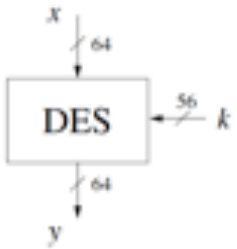
Data Encryption Standard (DES)

- Cifra de bloco por muito tempo mais usada no mundo
  - Após ter recomendação retirada, passou a ser usada na forma do triple-DES (que está para ser aposentado tb=)
- Pode-se dizer que é a mais estudada e conhecida
- Padronizada em 1977 pelo NBS (agora NIST)
  - FIPS PUB 46
- Encripta blocos de 64 bits usando chaves de 56 bits
- Enorme importância histórica
- Já não é considerada segura
  - Substituída pelo DES
  - Ainda em uso na forma de Triple-DES

História do DES

- IBM desenvolve a cifra Lucifer em 1971
  - Equipe liderada por Feistel
  - Bloco de 48, 32 or 128 bits
  - Chave de 48, 64 or 128 bits
- Em 1973, o NBS solicitou propostas para um novo padrão nacional de cifras
- A IBM submeteu uma versão revisada do Lucifer, que finalmente seria aceita como DES

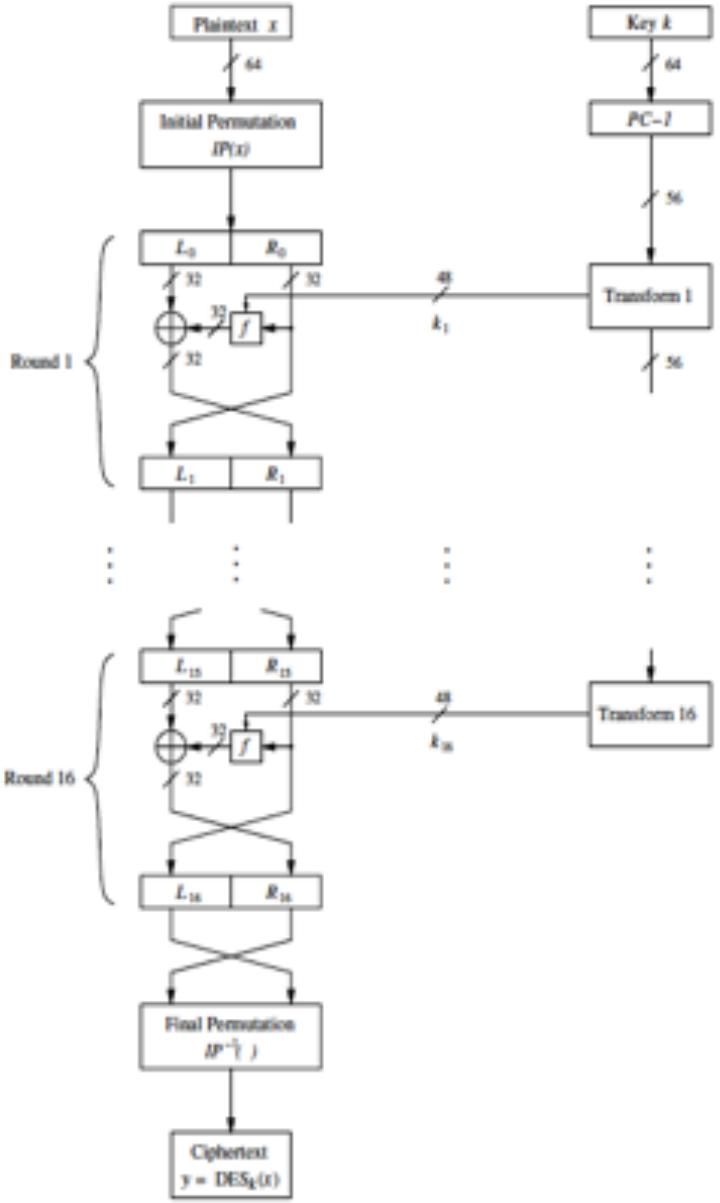
Estrutura do DES



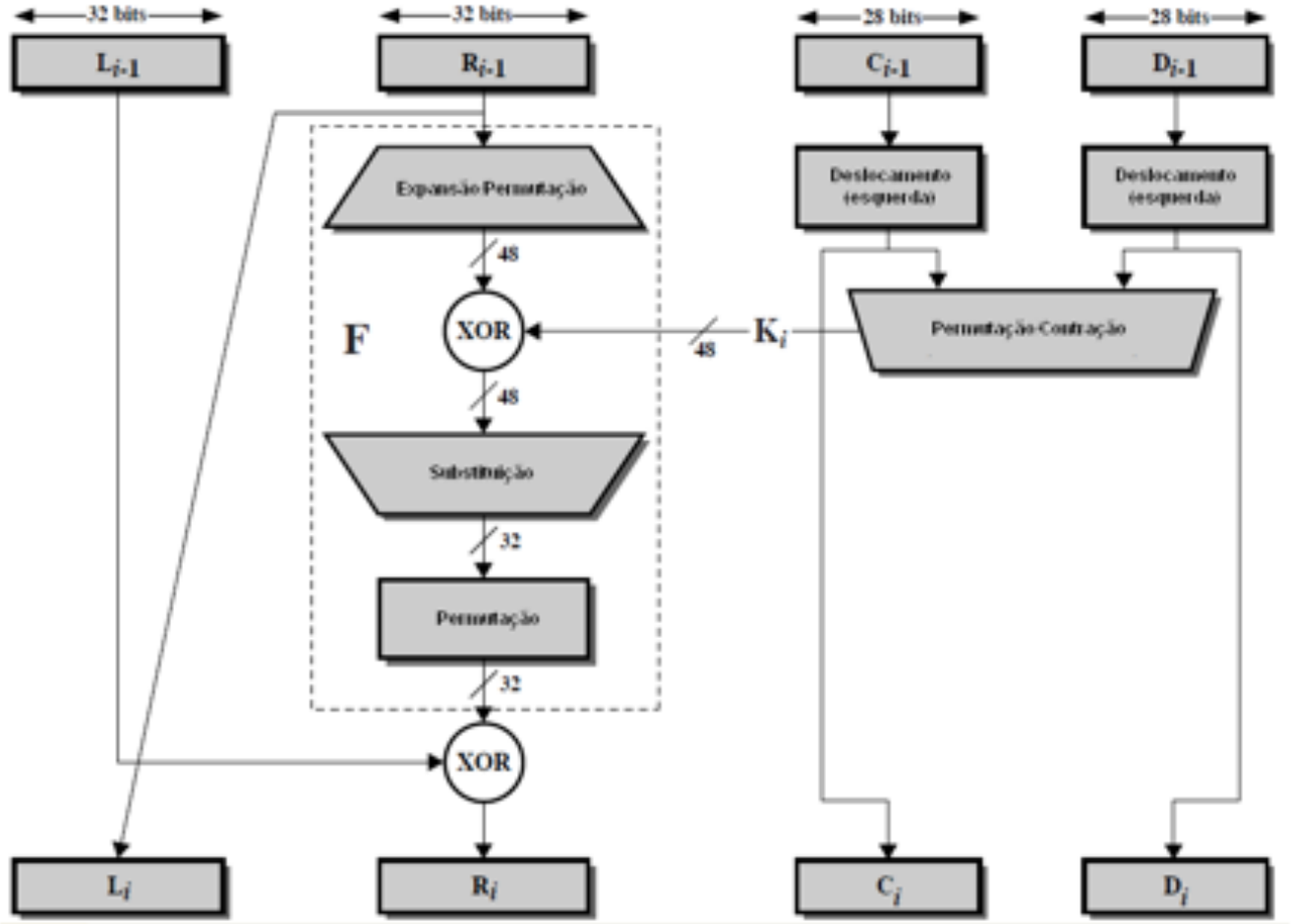
- Tamanho de bloco: 64 bits
- Tamanho de chave: 56 bits
  - (64 bits com 8 de paridade)
- Número de estágios: 16 rounds
  - 16 subchaves de 48 bits
  - Cada round é Feistel:

    $L_i = R_{i-1}$;

    $R_i = L_{i-1}$ XOR $f(R_{i-1},K_i)$, onde
    $f(R_{i-1},K_i) = P(S(E(R_{i-1})$ XOR $K_i))$



Round do DES


32 bits
32 bits
28 bits
28 bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Deslocamento (esquerda)
Deslocamento (esquerda)
Expansão Permutação
48
F
XOR
48
K_i
48
Permutação Contração
48
Substituição
32
Permutação
32
XOR
L_i
R_i
C_i
D_i

Triple DES

- Necessidade de substituição do DES
  - Diversos ataques demonstrados
  - Ataques de busca exaustiva de chave
- Possibilidade: usar múltiplas repetições do DES
- Double DES permite ataque "meet-in-the-middle"
- Três encriptações oferecem bem mais segurança

Triple DES

- Variação do DES – tripla encriptação com duas ou três chaves
- Padrão estabelecido em ANSI X9.17 & ISO 8732
- Ataques práticos ainda desconhecidos
  - Força-bruta bastante inviável
  - Ataque meet-in-the-middle com três chaves precisa de 2^{112} operações e 2^{56} memória
- Alternativa ainda popular

Dupla e tripla encriptações

- Dupla encriptação: $E(x) = E_{K_2}(E_{K_1}(x))$
- Tripla encriptação: $E(x) = E'_{K_3}(E'_{K_2}(E'_{K_1}(x)))$
  - E'_K pode denotar E_K ou $D_K = E_K^{-1}$
  - O caso $E(x) = E_{K_3}(D_{K_2}(E_{K_1}(x)))$ é denominado E-D-E tripla encriptação
    - O subcaso $K_1 = K_3$ é denominado tripla encriptação de duas chaves

Triple DES (cont.)

- Duas chaves
  - Seqüência E-D-E
  - $E(x)=E_{K_1}(D_{K_2}(E_{K_1}(x)))$
  - Padronizado em ANSI X9.17 e ISO8732
  - Sem ataques práticos conhecidos
- Três chaves
  - $E(x)=E_{K_3}(D_{K_2}(E_{K_1}(x)))$
  - Oferece maior segurança
  - Adotado por algumas aplicações Internet, como PGP e S/MIME

AES – Advanced Encryption Standard

- Uma substituição do DES mostrava-se necessária
  - Diversos ataques teóricos demonstrados
  - Diversos ataques de busca exaustiva de chave
- Triple-DES podia ser usado – mas era lento
- NIST efetuou uma "chamada de cifras" em 1997
- 15 candidatos aceitos em Junho de 1998
- 5 selecionados para fase seguinte em Agosto de 1999
- Rijndael selecionado como AES em Outubro de 2000
- Publicado como padrão FIPS PUB 197 em Novembro de 2001

Requisitos do AES

- Cifra de chave simétrica
- Blocos de 128 bits, chaves de 128/192/256 bits
- Mais rápido e forte que Triple-DES
- Vida útil de 20 a 30 anos
- Especificações completas e detalhes de projeto
- Implementações em Java e C

Critérios de avaliação AES

- Critério inicial:
  - segurança – esforço para criptanalisar
  - custo – computacional
  - Algoritmo e características de implementação
- Critério final:
  - Segurança geral
  - Facilidade de implementação (software e hardware)
  - flexibilidade

O selecionados do AES

- Lista de Agosto de 1999:
  - MARS (IBM) - complexo, rápido, alta margem de segurança
  - RC6 (EUA) - muito simples, muito rápido, pequena margem de segurança
  - Rijndael (Bélgica) - limpo, rápido, boa margem de segurança
  - Serpent (Europa) – limpo, lento, altíssima margem de segurança
  - Twofish (EUA) - complexo, muito rápido, alta margem de segurança

O selecionados do AES

- Diferenças-chave entre os selecionados
  - Estratégia de rounds
    - Poucos rounds complexos versus muitos rounds simples
  - Inovação
    - Redefinições de cifras existentes versus novas propostas

O AES – Rijndael

- Projetado por Rijmen-Daemen na Belgica
- Cifra iterativa, em vez de Feistel
  - Manipula dado em 4 grupos de 4 bytes
  - Opera o bloco inteiro em cada round
- Objetivos de projeto
  - Resistencia contra ataques conhecidos
  - Velocidade e código compacto em diversas CPUs
  - Projeto simples

Rijndael

- Processa blocos em quatro grupos de 4 bytes
- possui 9/11/13 rounds nos quais executa:
  - Substituição de bytes (um S-box para todos os bytes)
  - Deslocamento de linhas
  - Mistura de colunas
  - Adição (XOR) da subchave do round
- Possui um XOR inicial e o último round é incompleto
- Todas as operações podem ser combinadas em operações XOR e buscas em tabela
  - Bastante rápido e eficiente

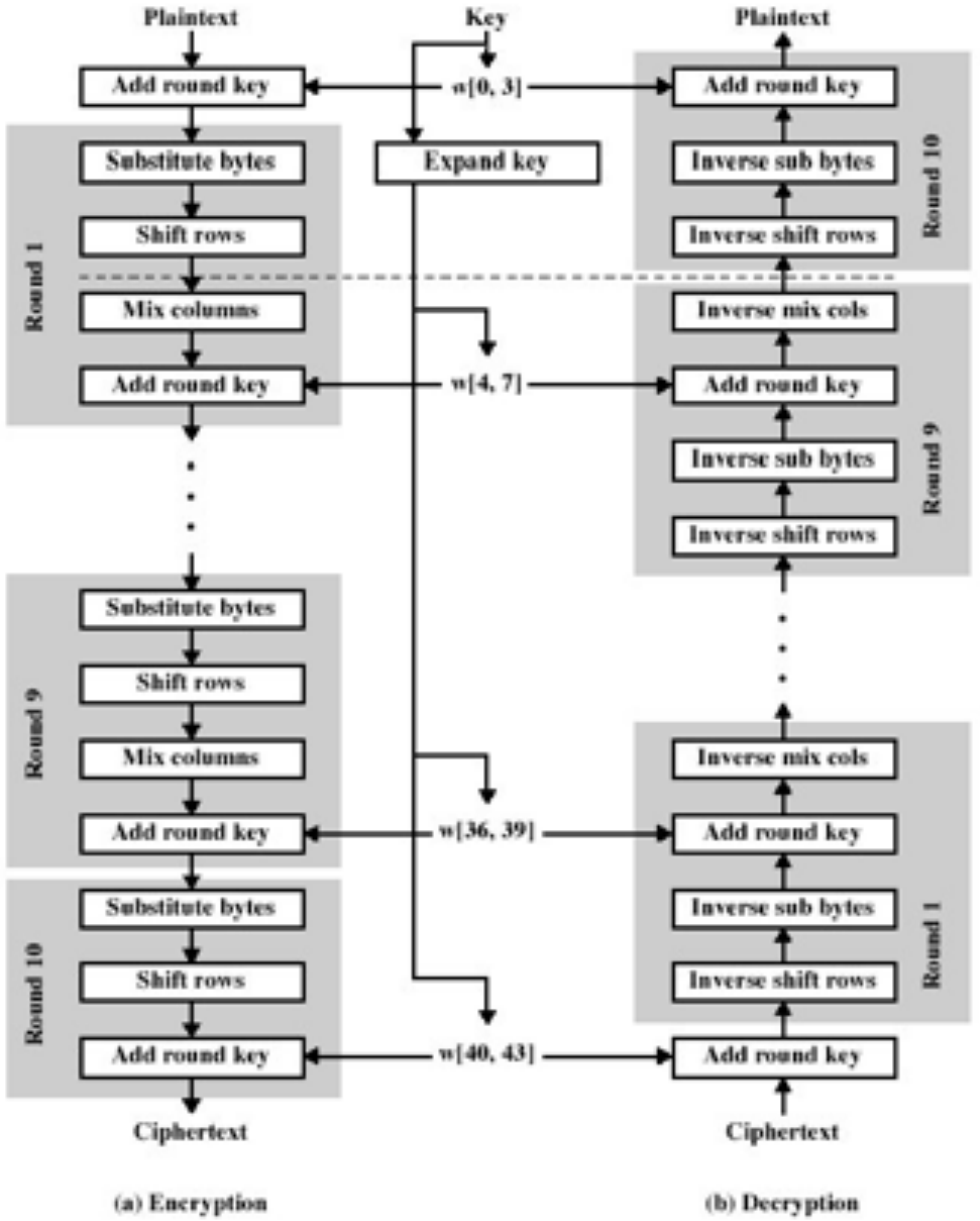
Aspectos de implementação

- Implementação eficiente em CPU 8 bits
  - Substituição de bytes usando tabela com 256 entradas
  - Deslocamento de linha é deslocamento de byte
  - Adição de chave é byte XOR
  - Mistura de colunas pode ser simplificada com busca em coluna

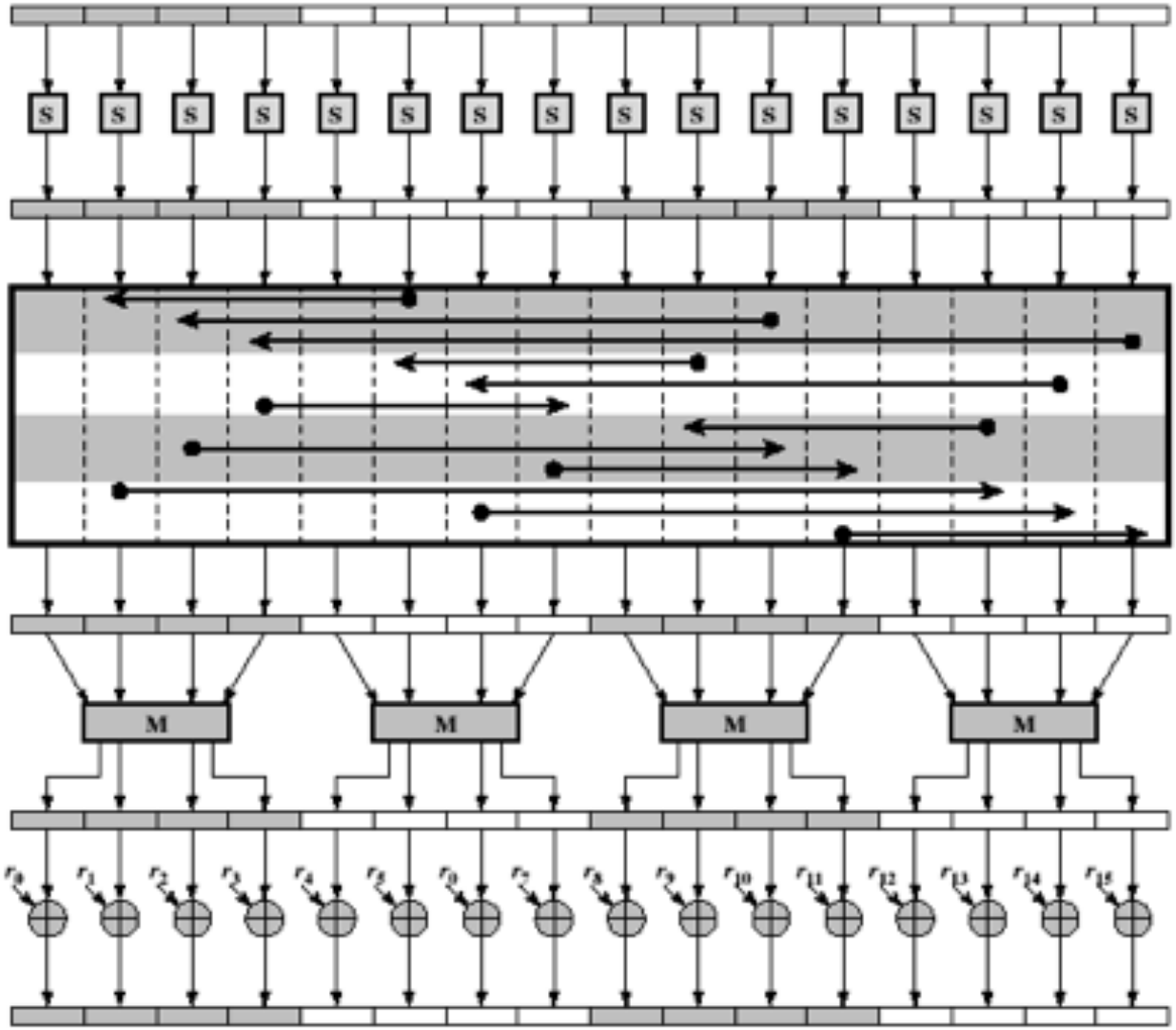
Aspectos de Implementação

- Implementação eficiente em CPU 32 bits
  - Redefina passos para usar palavras de 32 bits
  - precompute 4 tabelas de 256 palavras
  - Cada coluna em cada round pode ser precomputada usando 4 buscas em tabela + 4 operações XOR
  - Custo de 16Kb para armazenar tabelas
- Projetistas crêem que esta implementação eficiente foi decisiva na escolha do Rijndael

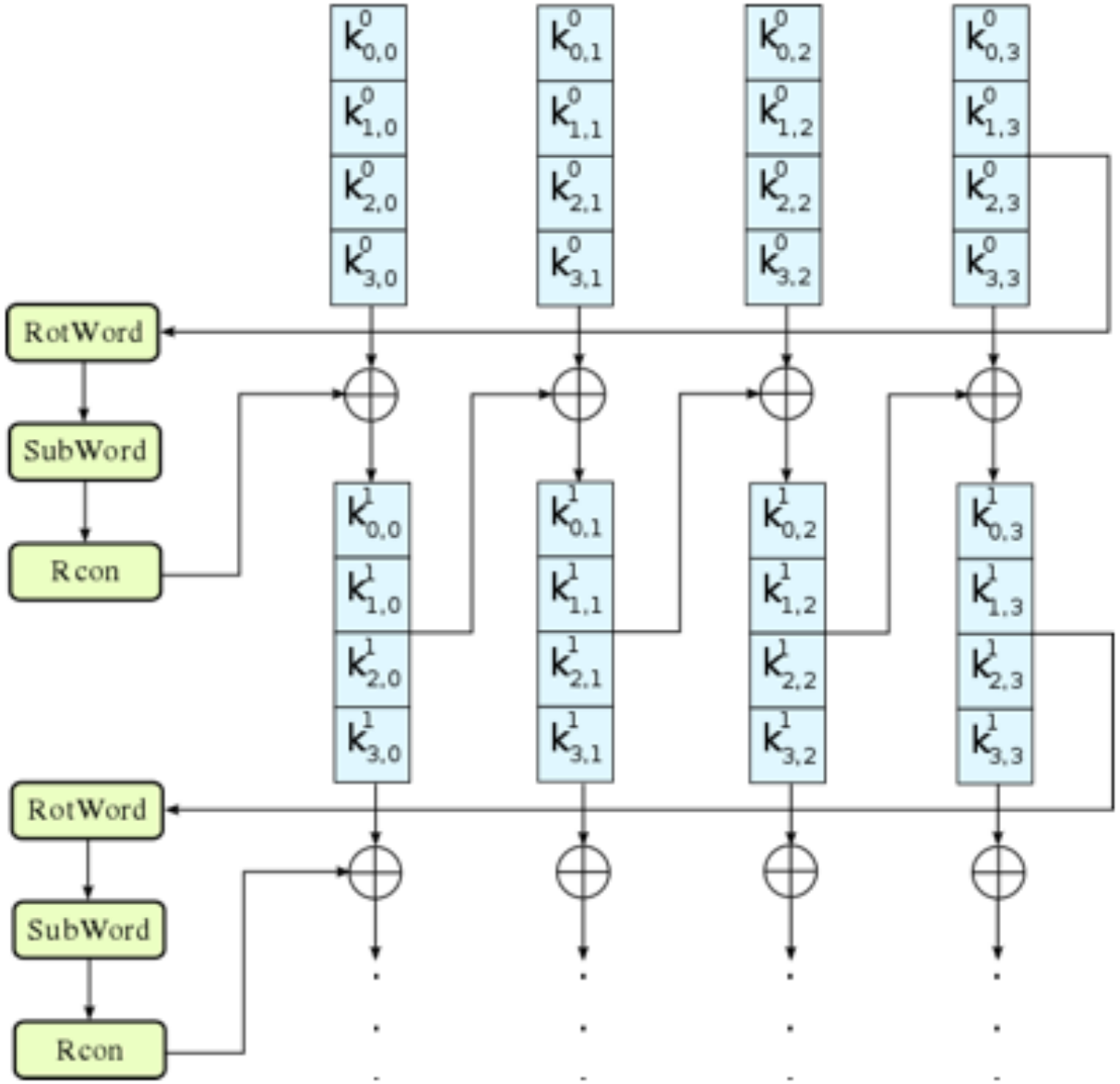
Estrurura do AES



Round AES



Key Schedule



Modos de operação de cifras

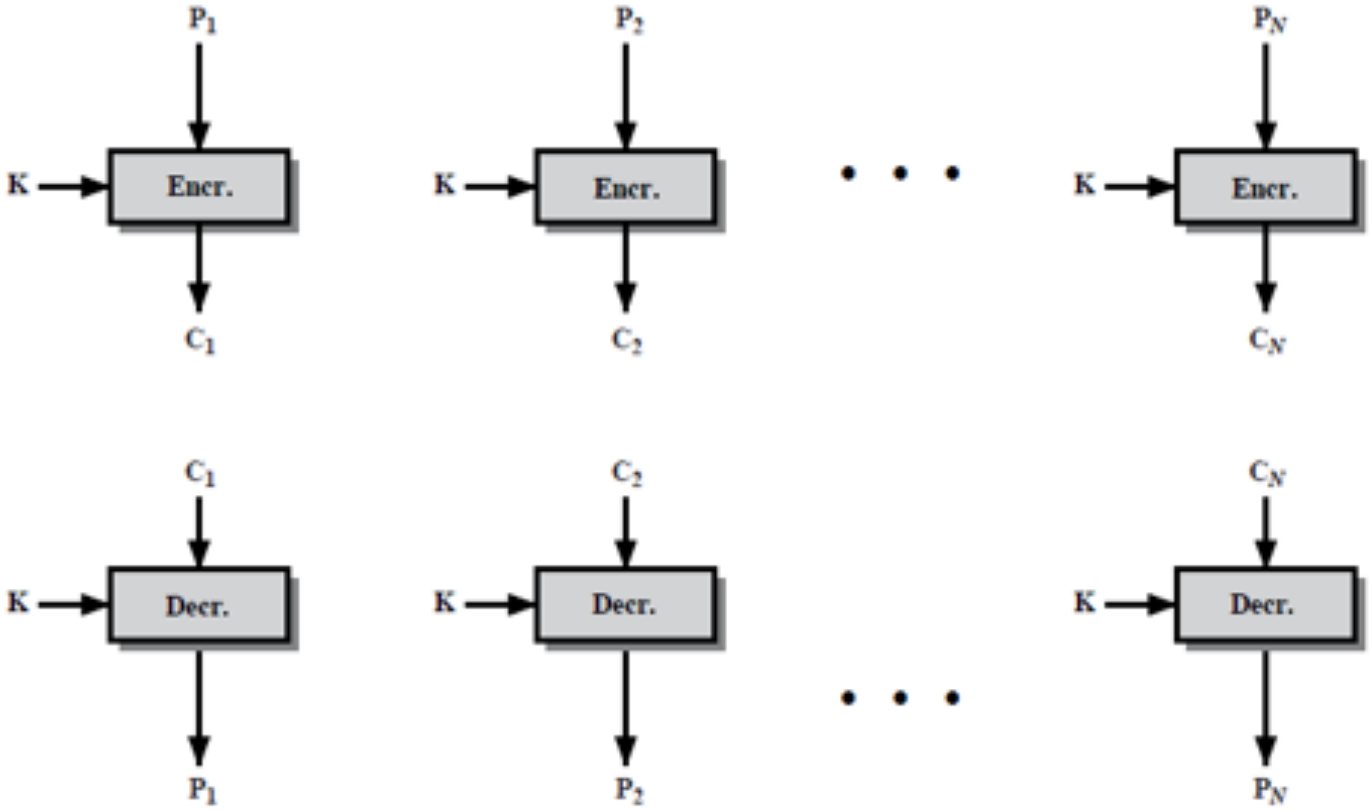
Modos de Operação

- Uma cifra de bloco define um conjunto de transformações indexadas por uma chave
- Cada bloco de n bits é levado em um outro bloco de n bits
- Quando a mensagem excede n bits, diversas abordagens são possíveis
  - Exemplo: quebrar as mensagens em blocos de n bits e encriptá-las individualmente

Modo ECB

- Electronic Codebook (é o exemplo anterior)
- Entrada:
  - Chave k
  - mensagem composta de t blocos de n bits, $m=x_1x_2...x_t$
- Saída: mensagem cifrada c1c2...ct
  - Onde $c_i:=E_k(x_i)$
  - Decriptação: $x_i:=E_k^{-1}(c_i)$
- Blocos idênticos, na mensagem plana, resultam em blocos idênticos, na mensagem cifrada
  - Reordenação dos blocos na mensagem plana provoca simples reordenação na mensagem cifrada

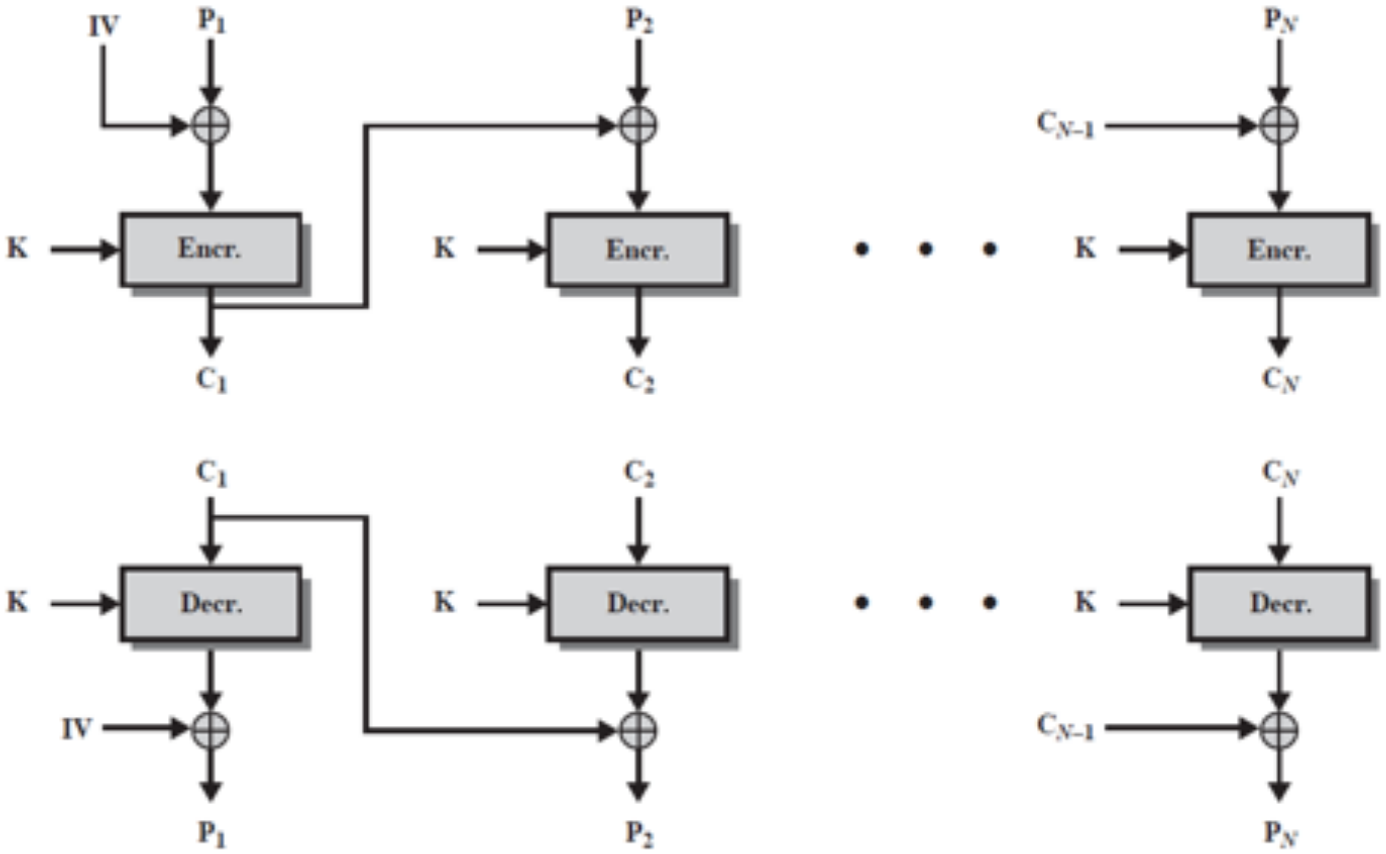
Modo ECB



Modo CBC

- Cipher Block Chaining
- Bloco cifrado depende do bloco cifrado anterior
- Entrada:
  - Chave *k*
  - mensagem composta de t blocos de n bits, $M=x_1x_2...x_t$
  - Inicialization vector IV de *n* bits
- Saída: mensagem cifrada $c_1c_2...c_t$
  - Onde $c_i:=E_k(x_i \oplus c_{i-1})$; $c_0=IV$
  - Decriptação: $x_i:=c_{i-1} \oplus E_k\text{-}1(c_i)$
- Rearranjo de blocos na mensagem plana determina conjunto diferente de blocos na mensagem cifrada

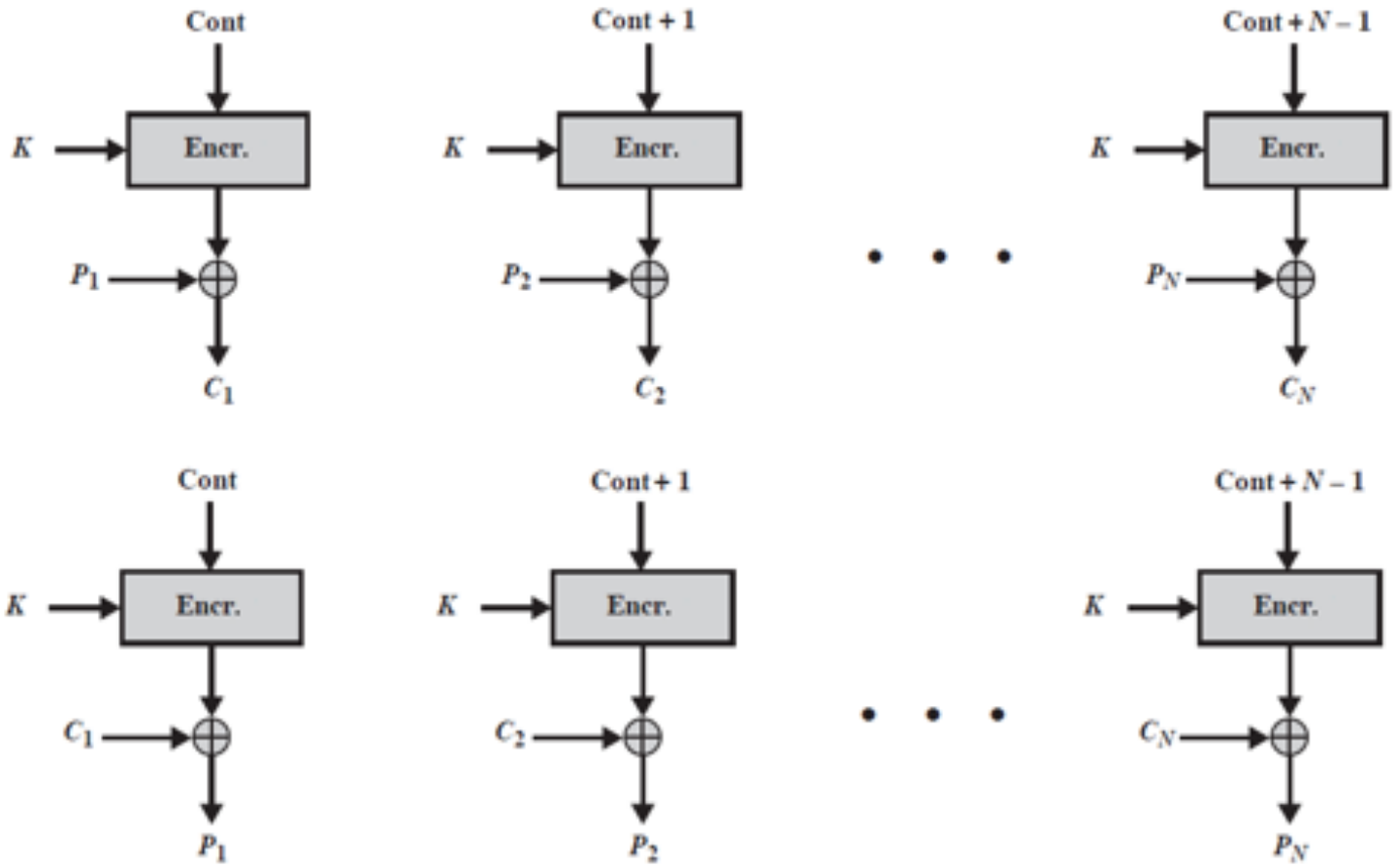
Modo CBC


IV
P1
P2
PN
CN–1
K
Encr.
K
Encr.
K
Encr.
C1
C2
CN
C1
C2
CN
K
Decr.
K
Decr.
K
Decr.
IV
CN–1
P1
P2
PN

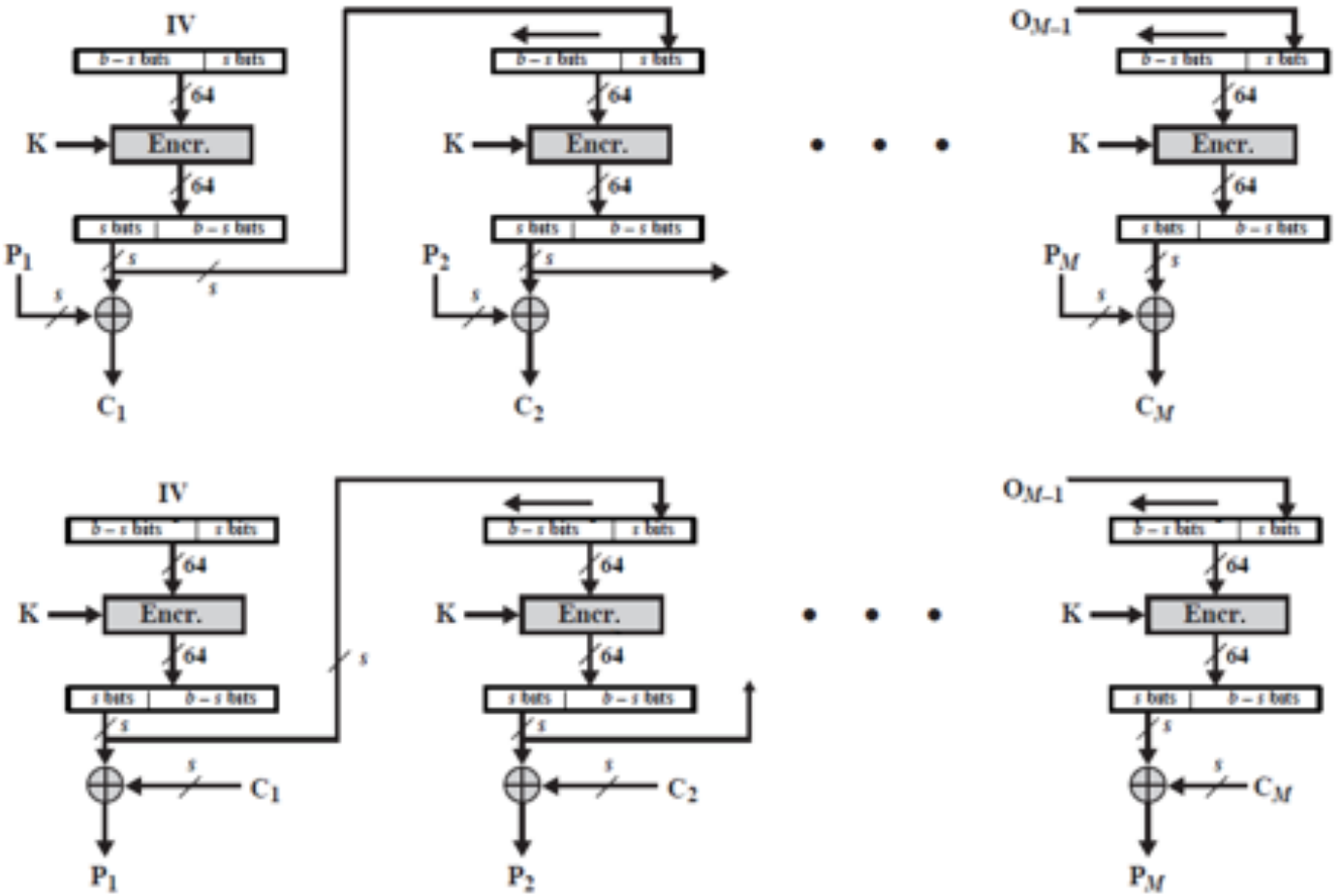
Modos stream: CTR, CFB e OFB

- Cifra é usada para gerar keystream que é combinada com a mensagem

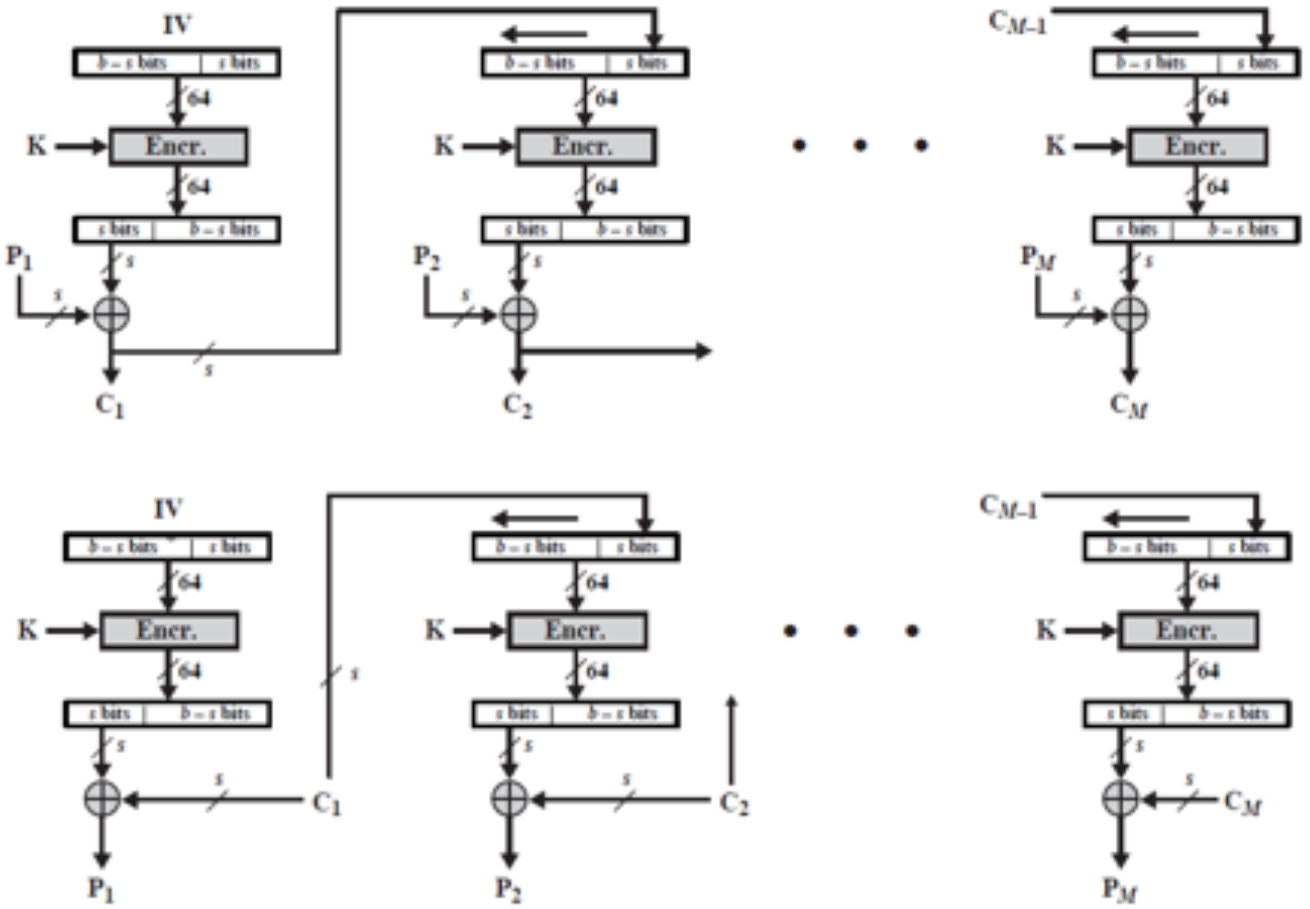
Modo CTR


Cont
K
Encr.
P_1
C_1
Cont + 1
K
Encr.
P_2
C_2
Cont + N – 1
K
Encr.
P_N
C_N
Cont
K
Encr.
C_1
P_1
Cont + 1
K
Encr.
C_2
P_2
Cont + N – 1
K
Encr.
C_N
P_N

Modo OFB



Modo CFB


IV
b – s bits
s bits
64
K
Encr.
64
s bits
b – s bits
P1
s
C1
P2
C2
CM–1
PM
CM
C1
C2
P1
P2
PM

Aplicações típicas dos modos

- Electronic Codebook
  - Transmissão de mensagens curtas
- Cipher Block Chaining
  - Uso geral orientado a bloco, autenticação
- Cipher Feedback
  - Uso geral orientado a stream
- Output Feedback
  - Uso orientado a stream em canais ruidosos (satélite)
- Counter Mode
  - Uso orientado a bloco com requisitos de alta velocidade