Universidade Federal do ABC

Segurança de Redes

Criptografia simétrica

Prof. João Henrique Kleinschmidt

Criptografia

- **Criptografia:**
  - Estudo dos princípios e técnicas pelas quais a mensagem ou informação pode ser transformada da sua forma original para outra forma que seja ilegível para úsuários não autorizados, mas possa ser conhecida por seu destinatário
- A criptografia é feita por algoritmos que:
  - Embaralham os bits dos dados ou mensagens
  - Podem utilizar uma ou mais chaves (ou par de chaves), dependendo do sistema criptográfico escolhido

Criptografia - Histórico

- Estudo da Escrita (*grafia*) Secreta (c*ripto*)
  - Cifragem utilizada na troca de mensagens
  - Em assuntos ligados à guerra , ao amor e à diplomacia
  - Primeiro uso documentado da criptografia:
    - 1900 a.c., no Egito
    - Uso de hieróglifos fora do padrão
- Entre 600 a.c. e 500 a.c.:
  - Hebreus utilizaram cifras de substituição simples para escrever o Livro de Jeremias
- Cifrador de Júlio César, aproximadamente 60 a.c.

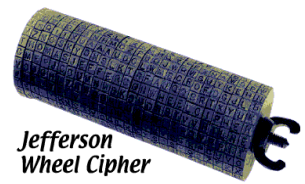
Histórico

- Dos anos 700 a 1200, são relatados estudos estatísticos, em que se destacam expoentes como al-Khalil, al-Kindi, Ibn Dunainir e Ibn Adlan

- Na Idade Média, a civilização árabe-islâmica contribuiu muito para os processos criptográficos, sobretudo quanto à criptoanálise

- Tratado sobre criptografia por Trithemius entre 1500 e 1600

- Thomas Jefferson e James Monroe cifravam as suas cartas para manter em sigilo as suas discussões políticas (1785) – roda criptográfica

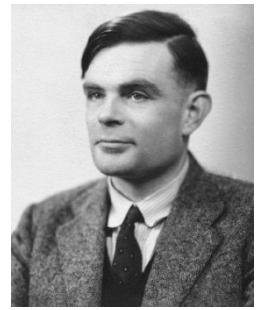


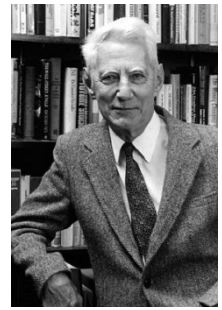
Histórico

- Em 1918, Arthur Scherbius desenvolveu uma máquina de criptografia chamada Enigma, utilizada amplamente pela marinha de guerra alemã em 1926, como a principal forma de comunicação
- A codificação da mensagem pelas máquinas Enigma era de difícil decodificação
  - Era necessário ter outra máquina idêntica
  - Saber qual a chave (esquema) utilizada para realizar a codificação

- Em 1928, o exército alemão construiu uma versão conhecida como “Enigma G”
  - Troca periódica mensal de chaves
  - Diferencial:
    - Máquina elétrico-mecânica, funcionando com três (inicialmente) a oito rotores
    - Aparentava ser uma máquina de escrever, mas quando o usuário pressionava uma tecla, o rotor da esquerda avançava uma posição, provocando a rotação dos demais rotores à direita, sendo que esse movimento dos rotores gerava diferentes combinações de cifragem

Histórico





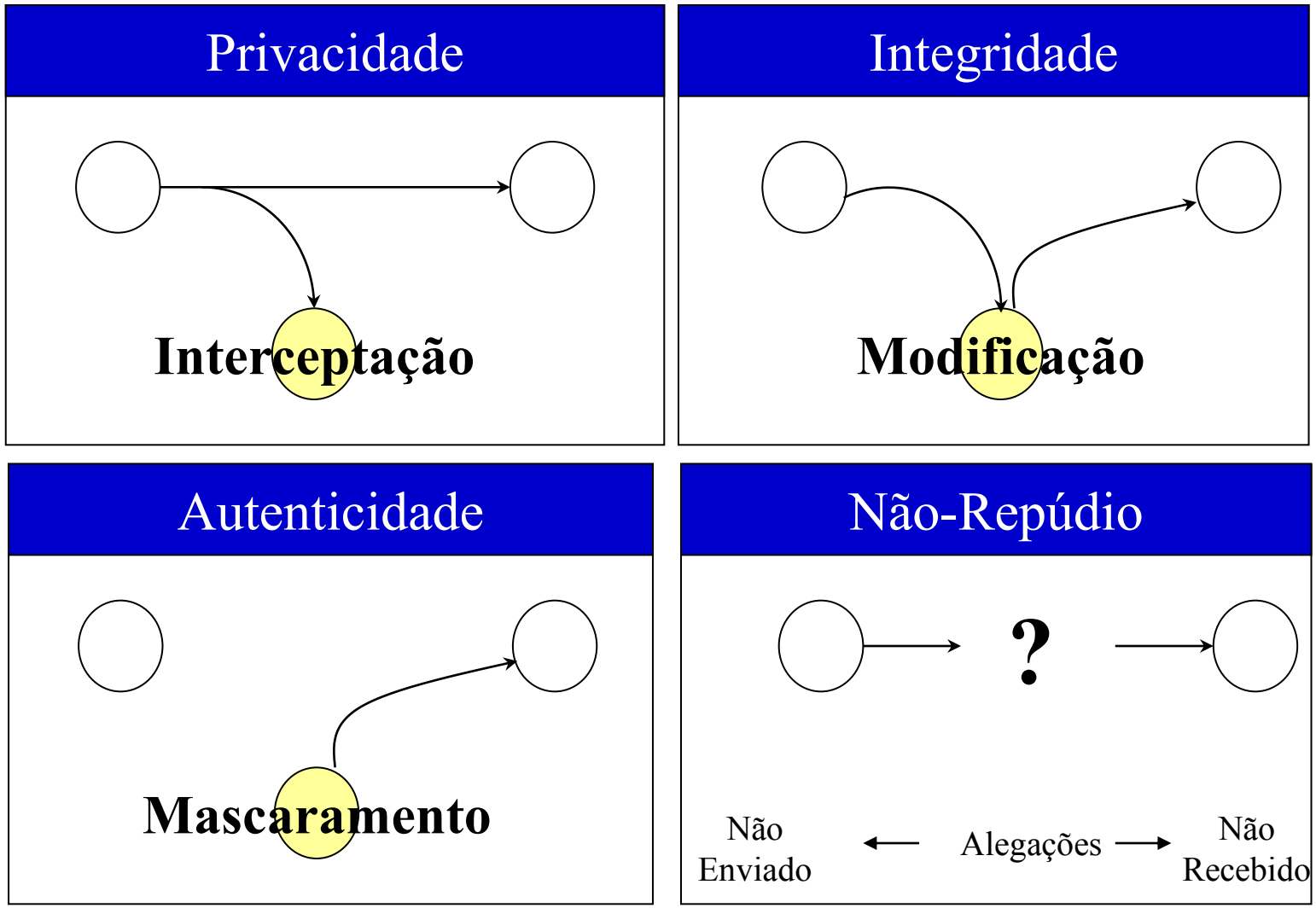
- Colossus:
  - Esforço de engenharia reversa das forças aliadas em decriptar as mensagens da marinha e do exército alemão
  - Êxito somente após se ter conseguido uma máquina Enigma alemã (furtada)
  - Alan Turing e colegas de “Bletchley Park” ajudaram a quebrar os códigos alemães
  - Foram inicialmente desenvolvidos como máquinas de decriptação, mas depois passaram a codificar mensagens das forças aliadas

- Devido aos esforços de guerra, a criptografia passou a ser largamente utilizada.
- Em 1948, Claude Elwood Shannon:
  - Desenvolveu a Teoria Matemática da Comunicação
  - Permitiu grandes desenvolvimentos nos padrões de criptografia e na criptoanálise
- Durante a chamada “Guerra Fria”, foram criados e utilizados diversos métodos a fim de esconder mensagens a respeito de estratégias e operações, criptografadas com diferentes métodos e chaves

Visão geral: objetivos

- A criptografia tem quatro objetivos principais:
  - *Confidencialidade* da mensagem
    - Só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada
  - *Integridade* da mensagem
    - O destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão
  - *Autenticação* do remetente
    - O destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem
  - *Não-repúdio* ou *irretratabilidade* do emissor
    - Não deverá ser possível ao emissor negar a autoria da mensagem.

Criptografia



Visão geral: objetivos

- Nem todos os sistemas ou algoritmos criptográficos são utilizados para atingir todos os quatro objetivos ao mesmo tempo
- Existem algoritmos específicos para cada uma destas funções
- Mesmo em sistemas criptográficos bem concebidos, bem implementados e usados adequadamente, alguns dos objetivos acima não são práticos ou desejáveis em algumas circunstâncias
  - Ex.:
    - O remetente de uma mensagem pode querer permanecer anônimo
    - O sistema pode destinar-se a um ambiente com recursos computacionais limitados

Criptografia

Exemplo de aplicação: Compra pela Internet

- Informação que permite a transação - valor e descrição do produto adquirido - precisa estar disponível no dia e na hora que o cliente desejar efetuá-la (**disponibilidade**).
- O valor da transação não pode ser alterado (**integridade**).
- Somente o cliente que está comprando e o comerciante devem ter acesso à transação (**controle de acesso**).
- O cliente que está comprando deve ser quem diz ser (**autenticidade**).
- O cliente tem como provar o pagamento e o comerciante não tem como negar o recebimento (**não-rejeição**).
- O conhecimento do conteúdo da transação fica restrito aos envolvidos (**confidencialidade**).

Texto plano e cifrado

- *Texto Plano –*
  - É um arquivo qualquer (mensagem, texto, imagem, etc) que é conteúdo legível para todos.
  - É sinônimo de Texto Aberto, Texto Claro ou Texto Legível.
- *Texto Cifrado –*
  - É resultado da passagem do Texto Plano por algum sistema criptográfico.
  - É sinônimo de Texto Criptografado, Texto Codificado.

Criptografia

- **Criptografia -** Ciência ou arte que dispõe de mecanismos para transformar um Texto Plano em um Texto Cifrado e vice-versa
- **Criptoanálise** - Ciência que estuda mecanismos para quebrar os textos cifrados, através de diversas técnicas e ferramentas de ataques a um sistema criptográfico
- **Criptologia** é Criptografia + Criptoanálise

Cifragem

- **Cifra**
  - Coleção **K** de funções inversíveis **e** e **d**, onde:
    e: M → C
    d: C → M, onde $\mathbf{d = e^{-1}}$ que é a função inversa de **e**
  - **M:** é o espaço de mensagens (espaço ≈ conjunto)
  - **C:** é o espaço de criptogramas (mensagens cifradas)
  - **K:** é o espaço de chaves
  - Pares **(e,d) ∈ K**, são pares de chaves
- **M** representa textos de uma linguagem **L**
- **∀ m ∈ M, ∀ e ∈ E**, temos que:
  - **e(m)=c** oculta o significado de **m** em **L**

Cifragem

- **Algoritmo Criptográfico**
  - Modelo de implementação, função **f**, onde:

  f: K x M ⟷ C, onde:

  - **f** executa encriptação:
    - Dado **(e,m)**, calcula **f(e,m) = e(m) = c**
  - **f** executa decriptação:
    - Dado **(d,c)**, calcula **f(d,c) = e^{-1}(c) = m**

Criptografia

- Exemplo:
- A Cifra de César (*Caeser Cipher*).
- Considerando as 26 letras do alfabeto (a,b,c,d,e,f,g,h,I,j,k,m,n,o,p,q,r,s,t,u,v,x,w,y,z), faz um deslocamento
- Neste método, com deslocamento=3, a se torna d, b se torna e, c se torna f, … …, z se torna c.
- Número de chaves: 25

Criptografia

- Exemplo:
- Substituição simples

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z
I	N	K	R	F	S	M	W	A	X	J	P	Z	Q	G	T	Y	B	D	E	O	H	V	L	U	C

- Número de chaves: 26!

Vulnerabilidade

- Frequência de letras na língua
- Sabe-se que vogais aparecem com mais freqüência
- No português:
  - Vogais:
  - Letra A (13,5%), E (12,5%), I (6%), O (5,5%) U(4,5%)
  - Consoantes:
  - Letra P (11,5%), T (9%), S (8%), D (5,5%), etc

- Permite o ataque estatístico!

Criptografia

- Cifra de Vigenère

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Chave é uma sequência de letras: Ex: ABC,CONA
- Transforma cada letra x_j do texto legível em outra letra $y_j=(x_j+c_j)\ mod\ 26$
- Número de chaves: 26^n

Alg. Restritos: Cifras de Substituição

1 - **Monoalfabética:**...M= $(\Sigma)^*$; Σ= *alfabeto de* **L**, f *substiui letra por letra em* m. Ex: Cifra de César: e = rotação de Σ = { ,a,b,...,z} em **e** posições.

2 - **Homofônica:**.....*monoalfabética contendo escolhas.*
(parecida com códigos de recuperação de erros)

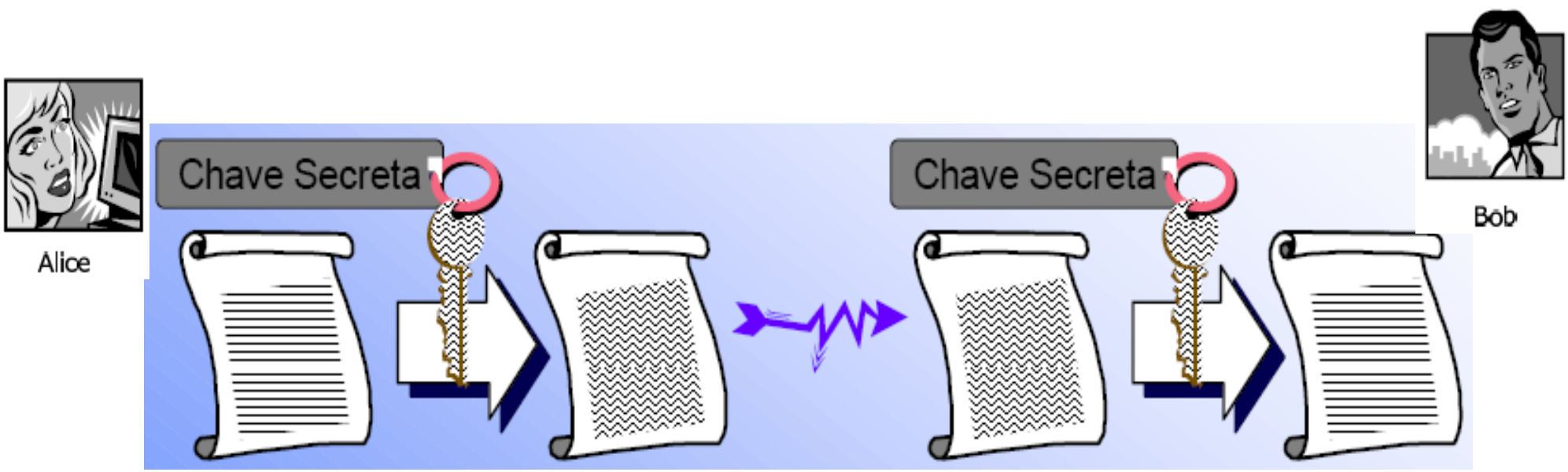
3 - **Poligrâmica:**.....M=C=$(\Sigma^n)^*$, Σ = *alfabeto de* **L**. f *substiui blocos de* n *letras*. Ex.: código de compactação de Huffman, onde Σ = {0,1}.

4 - **Polialfabética:**.....K=M=C=$(\Sigma^n)^*$, f *composta por* n *substituições monoalfabéticas (*n *é chamado* ***período*** *da cifra).*
Ex: Cifra Vigenère (1538): e = n distintas rotações, repetidas em bloco.
Ex: Vigenère com XOR: f= XOR da chave com blocos de n bytes

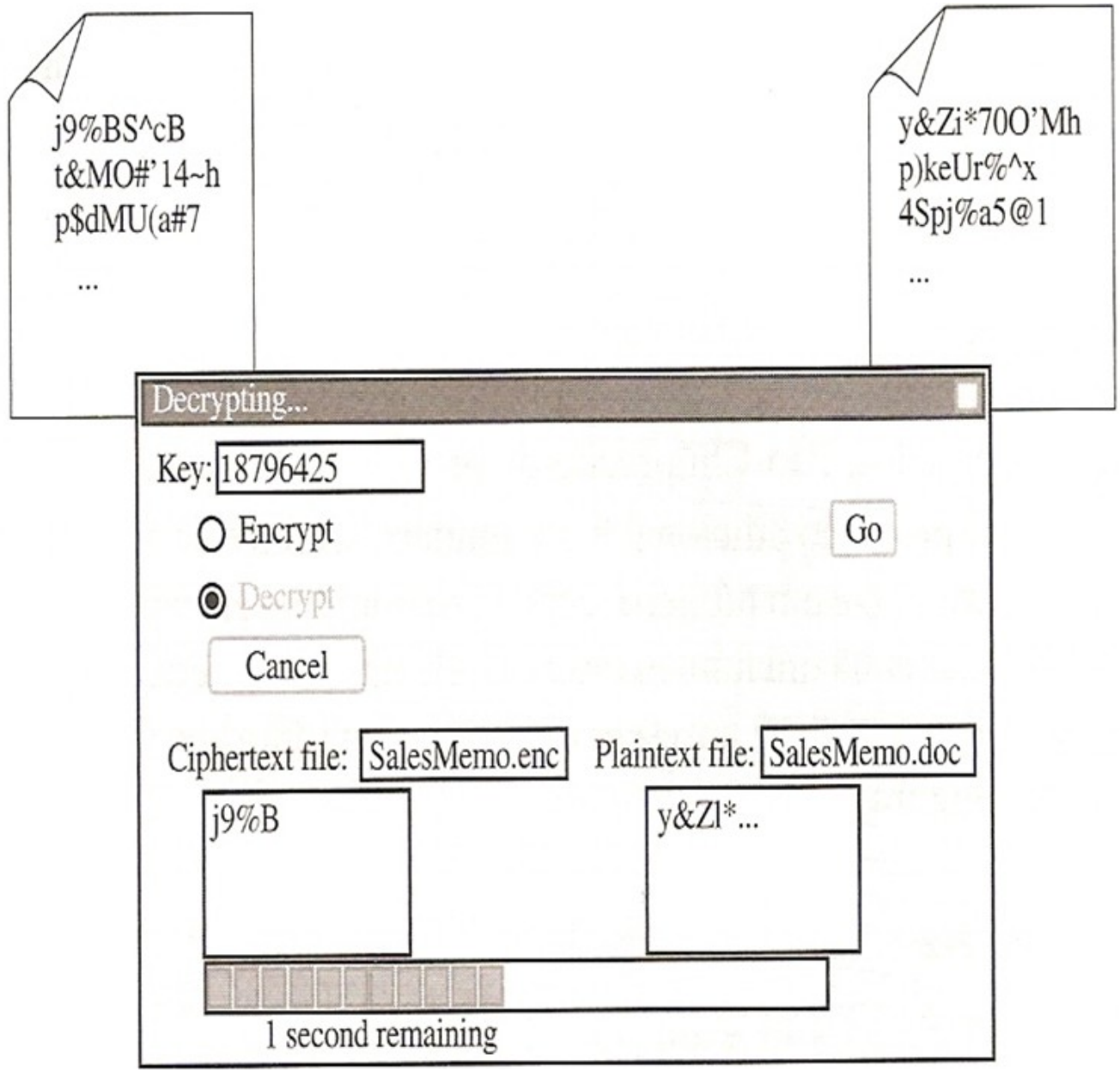
5 - **One-time pad:**.....*polialfabética onde* n *é limite para o tamanho das mensagens* m, *cada chave* **k** *é aleatória e usada apenas uma vez.*

Criptografia simétrica

- Uma mesma chave é usada para criptografar e decriptografar os dados.
- Vantagens: rápida
- Desvantagens: chave precisa ser transportada para o destino

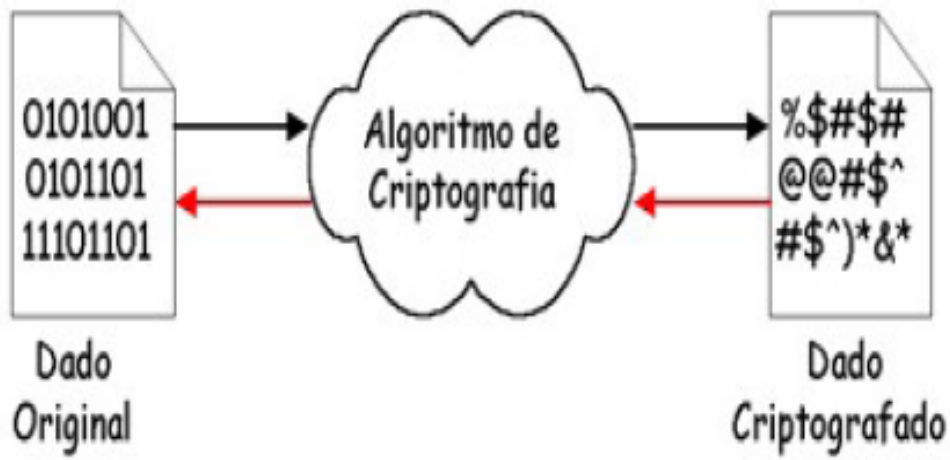


Se invasores tentarem outros números que não o valor secreto, eles obtêm apenas outras coisas sem sentido



Algoritmo criptográfico

- É uma função matemática utilizada para encriptação/decriptação.
- Se o algoritmo é secreto, o algoritmo é dito restrito.
- Na criptografia moderna, a segurança está baseada na chave utilizada e não no algoritmo.



Algoritmo criptográfico

- O algoritmo SEMPRE é descoberto!!!
- Ex: RC4, inventado em 1987 mas nunca publicado. Em 1994 foi descoberto por hackers. Atualmente é utilizado no Secure Socket Layer (SSL), protocolo de comunicação segura na Web.
- Algoritmos públicos são examinados pela comunidade de criptografia parar encontrar suas fraquezas.
- Um algoritmo secreto pode ter fraquezas conhecidas apenas pelos hackers!!!

Chave criptográfica

- É um número ou conjunto de números.
- O que é mais fácil? Proteger uma chave ou um algoritmo?
- Se um algoritmo é quebrado, todos os segredos são descobertos.
- Se uma chave é quebrada, apenas os dados protegidos por esta chave são descobertos.

Gerando uma chave

- Deve ser um número escolhido aleatoriamente.
- Se alguém souber os números atuais é possível prever os números seguintes? Então não é aleatório.
- Para saber se são números aleatórios:
  - Há aproximadamente a mesma contagem de “1s” e “0s” ?
  - Alguns padrões de “1s” e de “0s” aparecem com muita frequência?
- Impossível gerar números aleatórios num computador.
- Usar geradores de números pseudo-aleatórios (PRNG).
- O que torna esses números **pseudo-aleatórios** e **não aleatórios** é que eles **são repetíveis**.

Gerando uma chave

- Mas, **se os números são repetíveis**, **para que serve um PRNG** ?

- É que pode-se **alterar a saída** utilizando uma **entrada** (chamada de semente) que **precisamos nos certificar que essa entrada é alterada** todas as vezes que quisermos gerar novos números.

- Por que utilizar um PRNG e não apenas a semente ?

  - **Velocidade**. A coleção de sementes é um processo demorado.

  - **Entropia**. Quanto mais entropia na entrada, mais aleatória será a saída.

Atacando a chave

- Ataque de força bruta: testar todas as possibilidades.
- Chave de 40 bits: 0 a 1 trilhão
- Chave de 56 bits: 0 a 72 quatrilhões
- Cada bit adicionado dobra o número de chaves e o tempo gasto por um ataque de força bruta.
- Existem aproximadamente 2^{300} átomos no universo. Se cada átomo fosse um computador que verificasse 2^{300} chaves por segundo, levaria 2^{162} milênios para pesquisar 1% do espaço de uma chave de 512 bits.

Atacando a semente

- Em vez de reproduzir a chave, reproduzir o programa gerador e a semente.
- Se invasores adivinharem a semente, tentam reproduzir o gerador (PRNG) para criar a chave.
- Solução: uma boa semente.

- Semente da Netscape:
- Numa transação SSL, deve-se gerar uma chave. O gerador coletava como semente a hora do dia, o ID do processo e o ID do processo pai.
- Para obter a semente, foi feito um teste de força bruta no ID (15 bits) e a hora era facilmente obtida.
- Hoje: semente depende da posição do cursor, status da memória, último pressionamento da tecla, entre outros parâmetros.

Atacando o algoritmo

- Se certas combinações de bits aparecem no texto cifrado, uma parte correspondente do texto simples deve ter um outro padrão.

- Se o invasor adivinha o tipo do documento, como um memorando que contenha palavras como DE: José PARA: Maria

Força de um sistema criptográfico

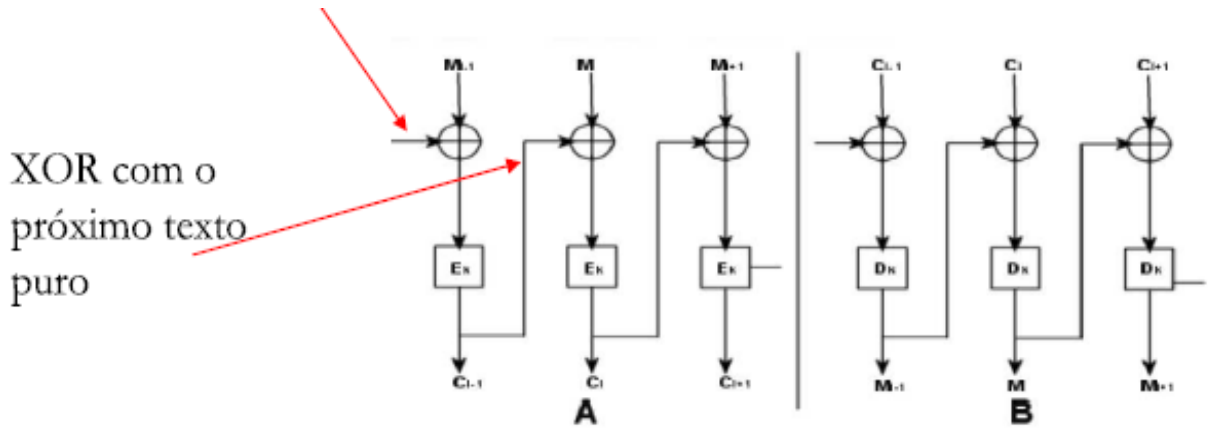
- A resistência a ataques depende de vários fatores:
  - Confidencialidade da chave
  - Dificuldade na determinação da chave (através de adivinhação ou tentativa de todas as possíveis chaves)
  - Dificuldade em inverter o algoritmo criptográfico sem o conhecimento da chave.
  - A possibilidade de se decodificar todo um texto cifrado dado que se saiba como parte dele é decodificada.
  - Conhecimento de propriedades peculiares da mensagem em texto claro que possam ser utilizadas para sua determinação.

Cifragem de bloco

- Texto simples dividido em blocos.
- ECB – *Electronic Code Book*
- Algoritmo opera sobre cada bloco de maneira independente.
- Blocos de 8 ou 16 bytes. Ex: num texto de 227 bytes dividido em blocos de 16 bytes, sobram 3 bytes. Deve preencher os 13 bytes restantes.
- Problema:
  - Se o mesmo bloco de texto simples aparece em dois lugares, o texto cifrado será o mesmo, criando um padrão de repetição.

Cifragem de bloco

- Para evitar cópias no texto cifrado
  - Modos de realimentação
- Cifragem de Blocos por Encadeamento (CBC) – *Cypher Block Chaining*
- Realiza operação XOR do bloco cifrado com o texto puro do próximo bloco.



Qualidade das cifras de bloco

Original

Usando ECB

Usando CBC

Cifragem de fluxo

- **Para encriptar:** a cifragem é feita bit a bit.

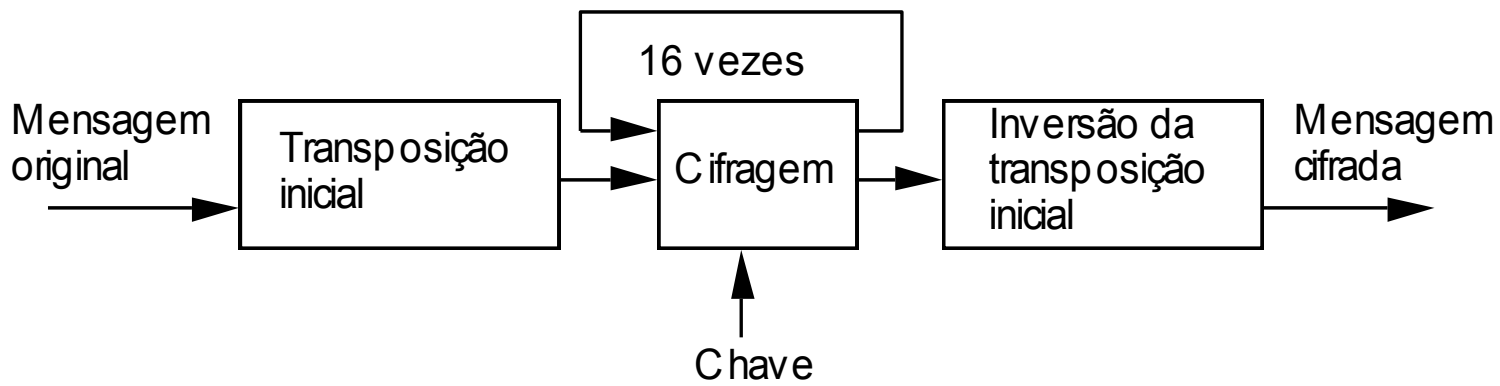
- Cifragem de fluxo mais rápida
- Padronização: bloco é mais utilizado
- Criptografia de arquivo e banco de dados: bloco
- Conexões seguras na web: fluxo

Padronização em Criptografia

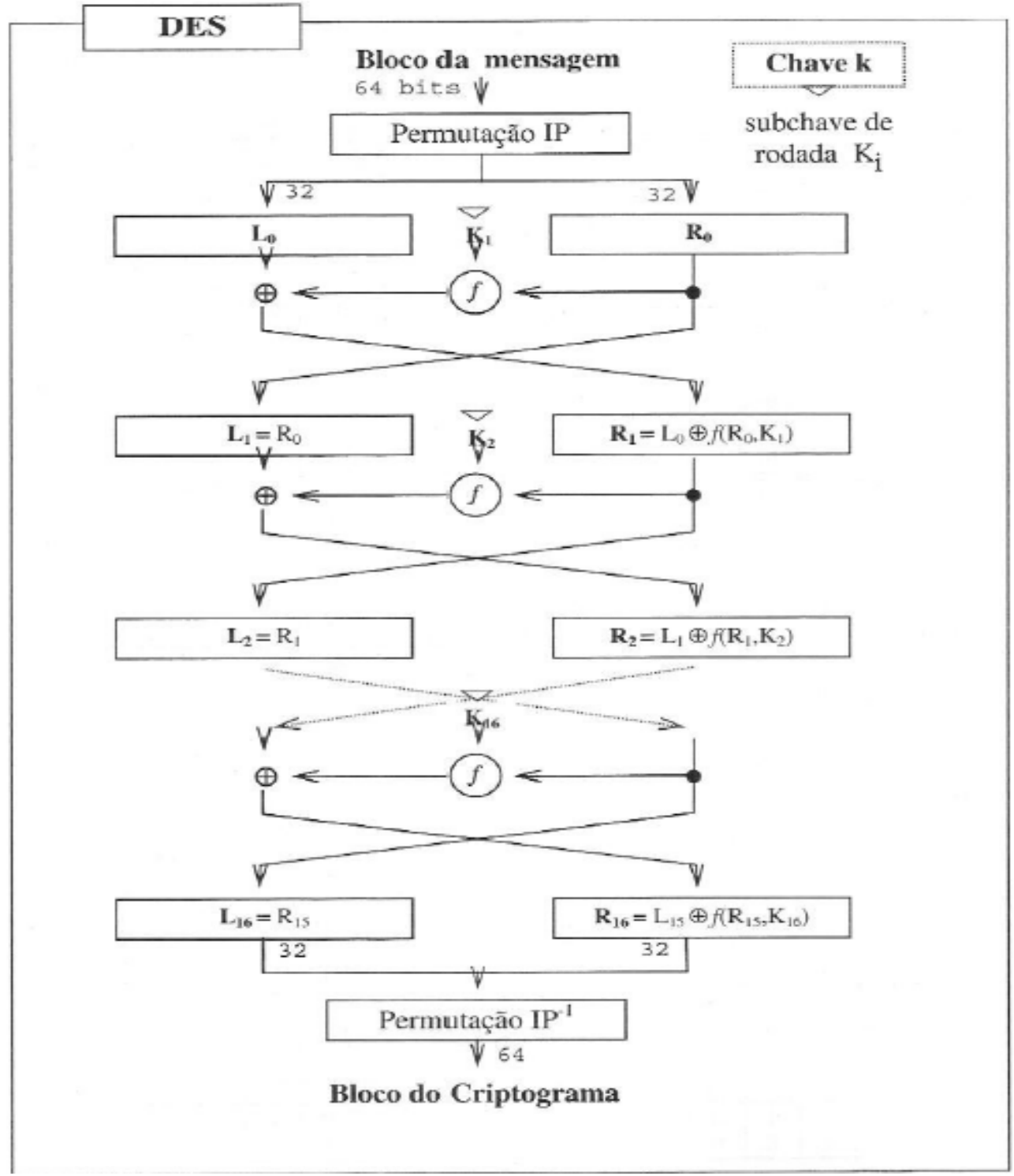
- Até 1970:
  - Não existiam padrões
- 1972:
  - *National Institute of Standards and Technology*, NIST
  - Programa para proteção a computadores e comunicação de dados
  - Estabelecimento de algoritmo criptográfico padrão para permitir interoperabilidade nas comunicações
- 1973:
  - NIST lança concurso para escolha de um algoritmo padrão (IBM: vence)
- 1976:
  - NIST lança o algoritmo padrão, com pequenas alterações, com o nome DES
  - DES: *Data Encription Standard*
- 1981-1992:
  - DES adotado também por ANSI e ISO

Digital Encryption Standard (DES)

- Cifragem de blocos de 64 bits com chave de 56 bits
- Em 1999, uma chave foi quebrada em menos de 24 horas
- Algoritmo:
  - Transposição inicial
  - 16 passos de cifragem que alternam
    - Substituição f
    - XOR
    - Permutação em sub-blocos L (Left), R (Right)
  - Transposição final
  - Para os 16 passos de cifragem utilizam-se 16 sub-chaves, todas derivadas da chave original

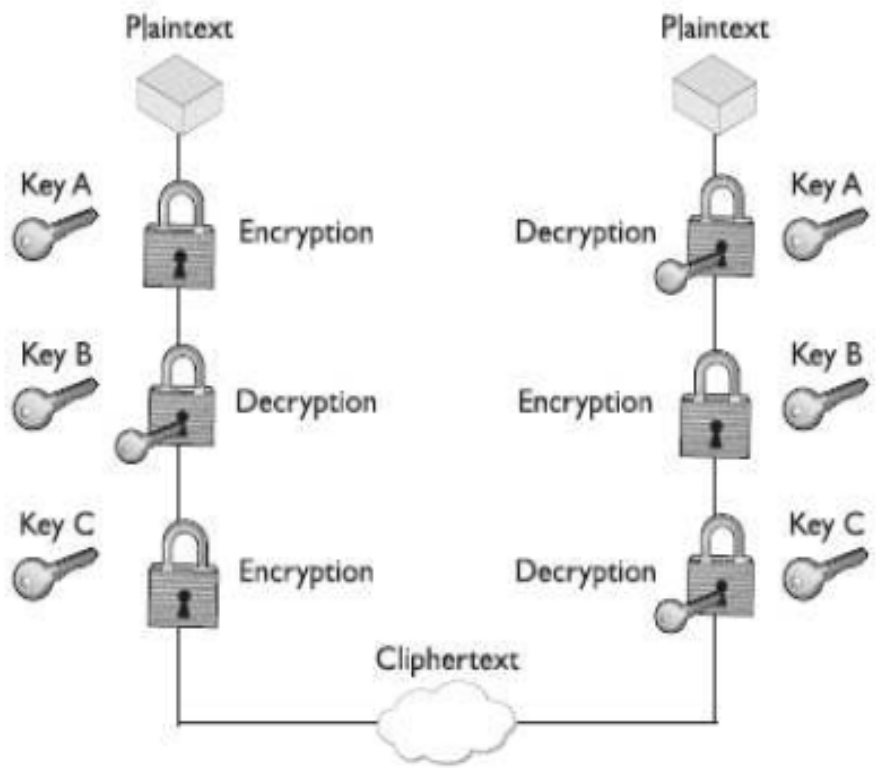


DES


DES
Bloco da mensagem
64 bits
Chave k
Permutação IP
subchave de rodada K_i
32
32
L_0
K_1
R_0
f
$L_1 = R_0$
K_2
$R_1 = L_0 \oplus f(R_0, K_1)$
$L_2 = R_1$
$R_2 = L_1 \oplus f(R_1, K_2)$
K_{16}
$L_{16} = R_{15}$
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$
32
32
Permutação IP^{-1}
64
Bloco do Criptograma

Triple DES

- Realiza 3 vezes o algoritmo DES
- O texto simples só aparece quando as três chaves forem corretas



Advanced Encryption Standard (AES)

- Resultado de um concurso de 4 anos
- Regras do concurso:
  - O algoritmo deveria ser uma cifra de bloco simétrica.
  - Todo o projeto deveria ser público.
  - Tamanho de chaves: 128, 192, 256 bits
  - Pode ser implementado em SW e HW.
  - O algoritmo deveria ser público ou licenciado em termos não-discriminatórios.
- Foram selecionados 15 candidatos (1998) e depois 5 finalistas (1999)
- Em outubro de 2000, o vencedor foi anunciado:
  - Algoritmo de Rijndael, criado por dois pesquisadores belgas: Vincent Rijmen e Joan Daemen
- Rápido o suficiente para codificar mais de 100 vídeos MPEG-2 em tempo real.
- Baseado na Teoria de Corpo de Galois (matemático francês).

Outros Algoritmos Simétricos

- NewDES (Robert Scott, 1985)
- RC4 (Ron Rivest, 1987)
- Khufu (Ralph Merkle, 1990)
- Khafre (Ralph Merkle, 1990)
- Skipjack (NIST, 1990)
- IDEA (Xuejia Lai & James Massey, 1991)
- MMB (John Daemen, 1993)
- GOST (USSR Gosudarstvenyi Standard, 1989)
- Blowfish (Bruce Schneier, 1994)
- RC5 w/r/b (Ron Rivest, 1995)
- ...

Projeto para Cifras de Bloco

- Princípios básicos
  - Considerar tempo computacional
  - Difusão
    - Espalhamento de bits da chave ou da mensagem
  - Confusão
    - Ocultação da relação entre mensagem, criptograma e chave
    - Dificultar a análise estatística

Gerenciamento de chave simétrica

- A criptografia de chave simétrica pode manter seguro seus segredos, mas pelo fato de **precisarmos das chaves para recuperar os dados criptografados, devemos mantê- las** seguras.
- Soluções para o **armazenamento de chaves podem ser dispositivos** pequenos, projetados para proteger chaves ou senhas.
- Ou utilizar **criptografia de chave simétrica para proteger os** megabytes de informação e alguma técnica para proteger chaves.

Armazenamento de chaves em hardware

- Tokens
  - Um cartão inteligente
  - Um pequeno anexo da porta USB
  - Um anel de dedo
- A vantagem de se utilizar tokens é que **um invasor não tem acesso a eles.**
- Quando precisar utilizar uma chave simétrica, transfere-se a chave do token para o computador.
- Tokens podem armazenar senhas de várias contas.
- Utilizar um token para gerar grandes senhas aleatórias e para armazenar essas senhas.
- Não é preciso lembrar da senha.

Aceleradores de criptografia

- Funcionam o tempo todo conectados, internos ou externos ao computador.
- Aceleradores de criptografia são construídos de tal modo que seu espaço de armazenamento não é visível.
- A maioria dos aceleradores funcionam conjuntamente com um token. Não operam sem que um token seja inserido, com uma senha correta.
- Para encriptar dados, deve-se obter a chave do *token.* Com um acelerador, envia-se o texto simples ao dispositivo, ele o criptografa e retorna o texto cifrado.