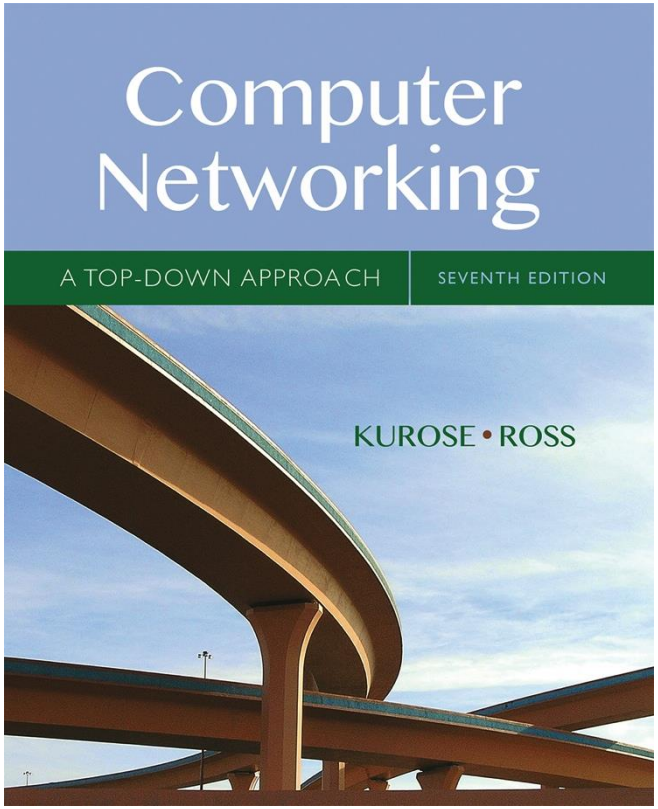
PTC 2550 - Aula 19

5.1 O que é segurança de rede?
5.2 Princípios de criptografia

(Kurose, p. 587 - 626)
(Peterson, p. 444-454)

09/06/2017

Capítulo 5
Segurança



Computer Networking: A Top Down Approach, Cap. 8

Chapter 5: Segurança de rede

Objetivos do capítulo:

- entender princípios de segurança de rede:
  - criptografia e seus *muitos* usos além da "confidencialidade"
  - autenticação
  - integridade de mensagens
- segurança na prática:
  - *firewalls* e sistemas de detecção de intrusão
  - segurança nas camadas de aplicação, transporte, rede e enlace

Capítulo 5 - Sumário

5.1 O que é segurança de rede?

5.2 Princípios de criptografia

5.3 Integridade de mensagem, autenticação

5.4 Tornando o e-mail seguro

5.5 Tornando conexões TCP seguras: SSL

5.6 Segurança na camada de rede: IPsec

5.7 Tornando LANs sem fio seguras

5.8 Segurança operacional: *firewalls* e IDS

O que é segurança de rede?

confidencialidade: apenas transmissor e receptor desejadp devem "entender" conteúdo da mensagem

- transmissor criptografa mensagem
- receptor decripta mensagem

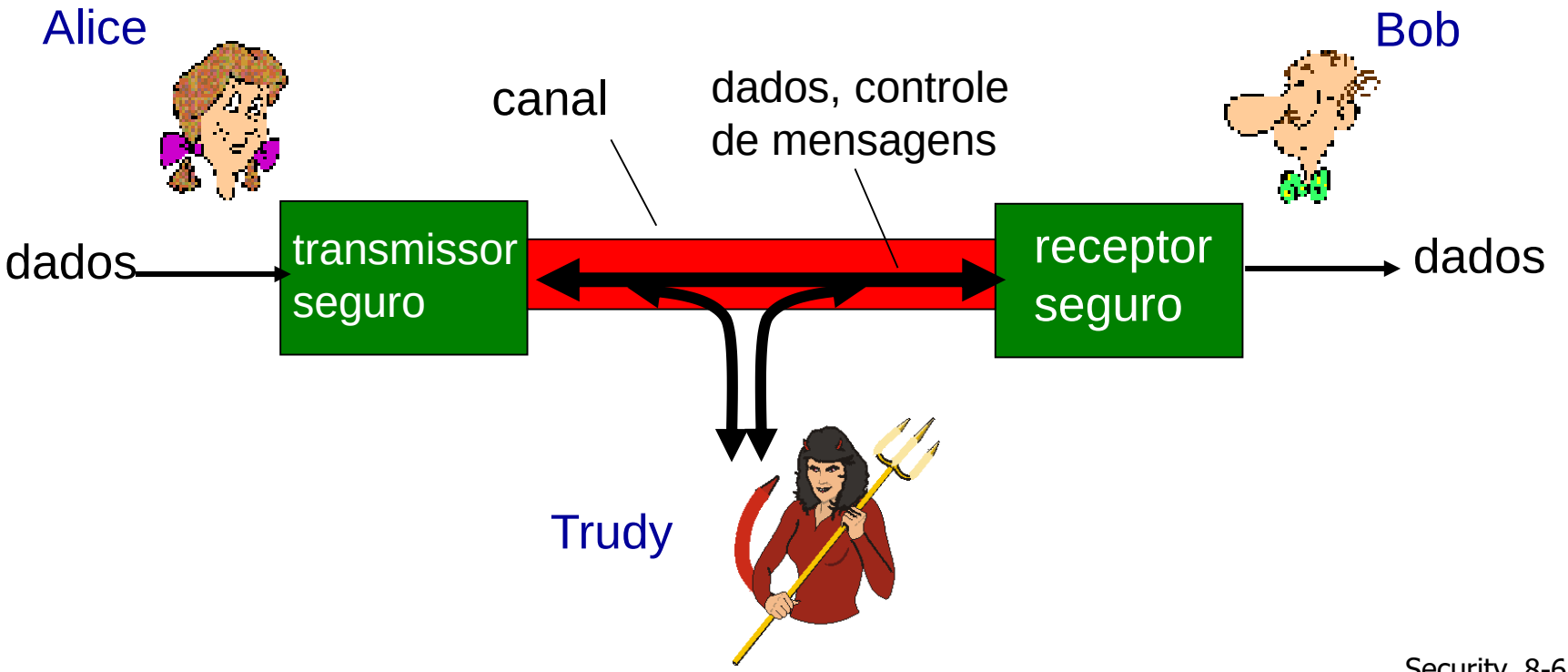
autenticação: transmissor e receptor querem confirmar identidade um do outro

integridade da mensagem: transmissor e receptor querem ter certeza de que mensagem não foi alterada (em trânsito ou depois) de forma não detectada

acesso e disponibilidade: serviços precisam ficar acessíveis e disponíveis a usuários

Amigos e inimigos: Alice, Bob, Trudy

- Nomes conhecidos no mundo da segurança de rede...
- Bob, Alice querem se comunicar "de forma segura"
- Trudy (intruso) pode tentar interceptar, apagar ou adicionar mensagens



Quem poderiam ser Bob e Alice?

- Bobs e Alices da vida real:
- navegador e servidor web para transações eletrônicas (exemplo, compras *on-line)*
- cliente e servidor de banco *on-line*
- servidores DNS
- roteadores trocando atualizações de tabelas de roteamento
- outros exemplos?

O que a Trudy pode fazer?

Q: O que a Trudy pode fazer?

A: Muita coisa!

- *Espionar:* interceptar mensagens
- ativamente *inserir* mensagens na conexão
- *Personificar:* pode falsificar (*spoof*) o endereço de origem no pacote (ou qualquer campo no pacote)
- *Sequestrar:* "assumir o controle" de uma conexão em andamento removendo transmissor ou receptor, inserindo-se no lugar
- *denial of service:* impedir que o serviço seja usado por outros (por exemplo, sobrecarregando recursos)

❖ Banco de dados de vulnerabilidades CERT

Capítulo 5 - Sumário

5.1 O que é segurança de rede?

5.2 Princípios de criptografia

5.3 Integridade de mensagem, autenticação

5.4 Tornando o e-mail seguro

5.5 Tornando conexões TCP seguras: SSL

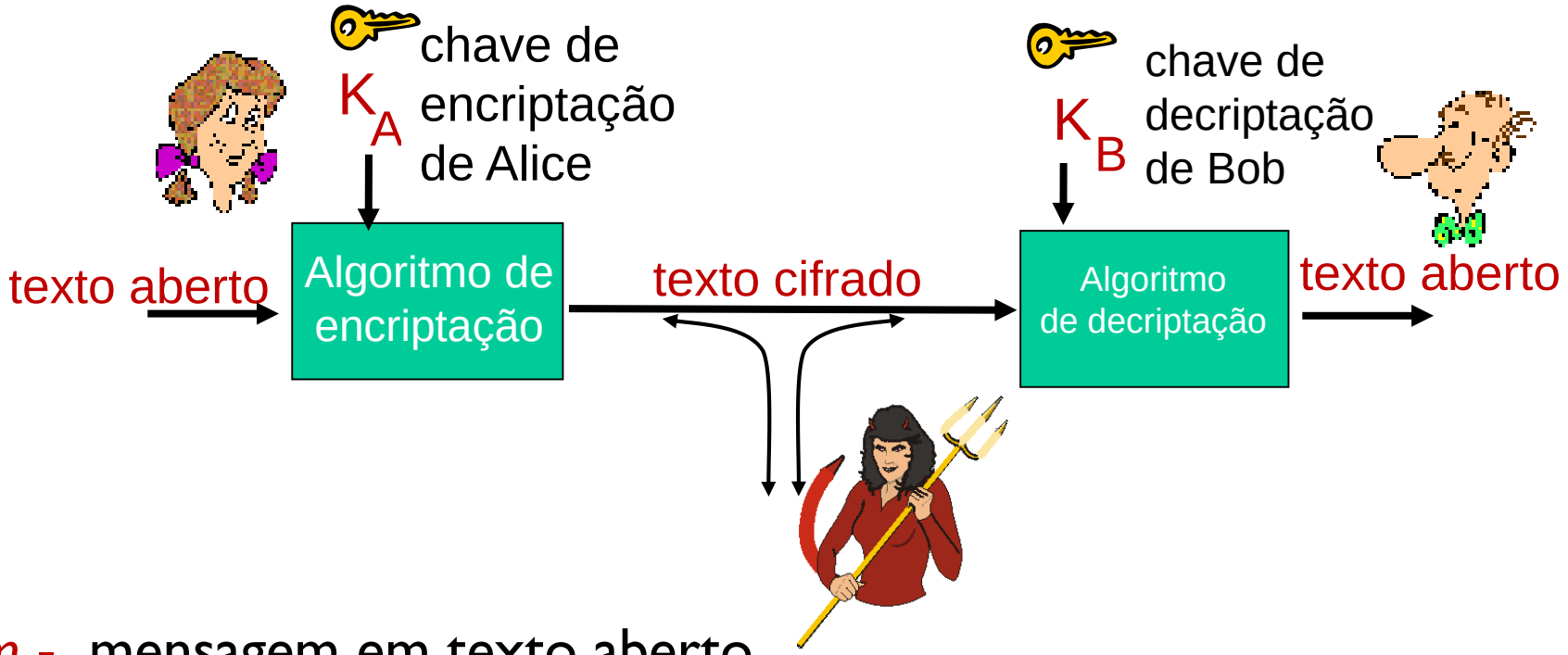
5.6 Segurança na camada de rede: IPsec

5.7 Tornando LANs sem fio seguras

5.8 Segurança operacional: *firewalls* e IDS

A linguagem da criptografia

Algoritmos de encriptação usuais são públicos e disponíveis: MD5, RSA, 3DES, AES, etc. Segredo está nas chaves…



m - mensagem em texto aberto

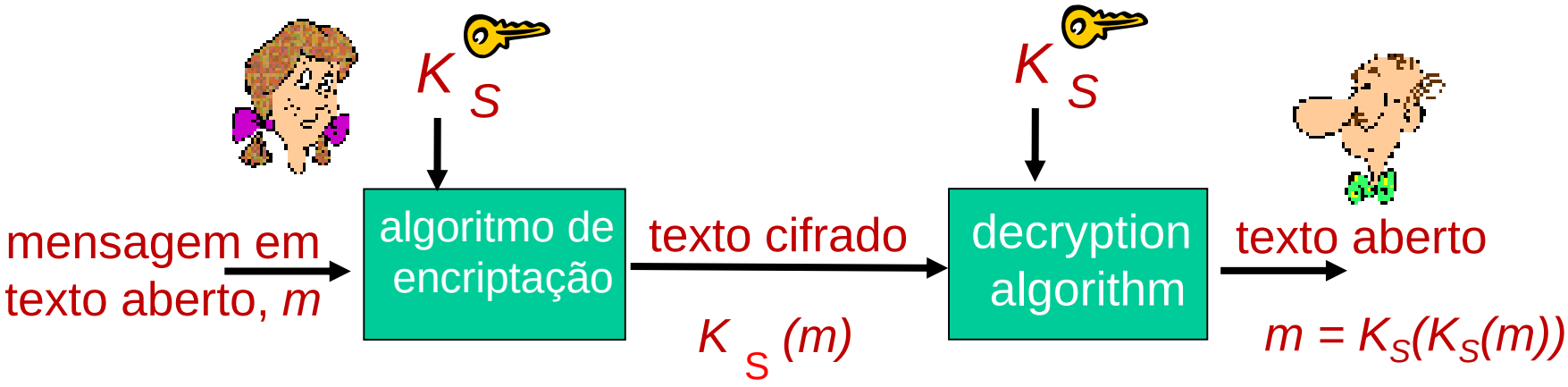
$K_A(m)$ - texto cifrado, criptografado com a chave K_A

$m = K_B(K_A(m))$

Algoritmos de criptografia

- 2 grandes grupos de algoritmos
  - Sistemas de chave simétrica
    - Chaves de Alice e Bob são idênticas e secretas
  - Sistemas de chave pública
    - Par de chaves é usado – uma é conhecida público (inclusive Alice e Bob) e a outra é conhecida apenas por Alice ou Bob (mas não por ambos)

Criptografia de chave simétrica



criptografia de chave simétrica: Bob e Alice compartilham chave (simétrica): K_S

- por exemplo, chave é saber padrão de substituição em algoritmo de substituição monoalfabético

Q: Como Bob e Alice entram em acordo sobre a chave?

Sistema de encriptação simples

Algoritmo de substituição: substituir um "símbolo" por outro

- algoritmo monoalfabético: substitui diretamente uma letra por outra

```
plaintext:   abcdefghijklmnopqrstuvwxyz
             |                       |
             v                       v
ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

Exemplo:

```
Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Chave de encriptação: mapeamento do conjunto de 26 letras em outro conjunto de 26 letras

Perguntas: Quantas chaves diferentes existem? Seguro?

Quebrando um esquema de encriptação

- Ataque com texto cifrado apenas: Trudy tem apenas texto cifrado que ela pode analisar
- 2 abordagens:
  - força bruta: procurar entre todas as chaves
  - análise estatística

- ataque com texto aberto conhecido: Trudy tem texto aberto correspondente ao texto cifrado
  - por exemplo, no algoritmo monoalfabético, Trudy descobre os correspondentes para a,l,i,c,e,b,o,
- ataque com texto aberto escolhido: Trudy consegue obter texto cifrado para texto aberto escolhido

Um algoritmo de encriptação mais sofisticado

- *n* cifras de substituição, $M_1,M_2,\ldots,M_n$
- padrão cíclico:
  - por exemplo, *n=4*: M_1,M_3,M_4,M_3,M_2; M_1,M_3,M_4,M_3,M_2; ..
- para cada novo símbolo em texto aberto, usar padrão de substituição subsequente no padrão cíclico
  - USP: U de M_1, S de M_3, P de M_4

Chave de encriptação: n cifras de substituição e padrão cíclico

- chave não precisa ser apenas padrão de *n*-bits

Algoritmos de chave simétrica atuais

- *2 grandes grupos:*

  - Algoritmos de blocos (*block ciphers*)
    - PGP (email), SSL (TCP), IPsec(transporte na camada de rede)
    - Mensagem processada em blocos de *k* bits
    - Bloco de *k* bits de texto aberto é mapeado em bloco de *k* bits de texto cifrado
    - Vamos estudar esses com mais detalhes

  - Algoritmos de fluxo (*stream ciphers*)
    - LANs sem fio

Exemplo 1

- *Algoritmo de bloco com k=3*

input	output	input	output
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

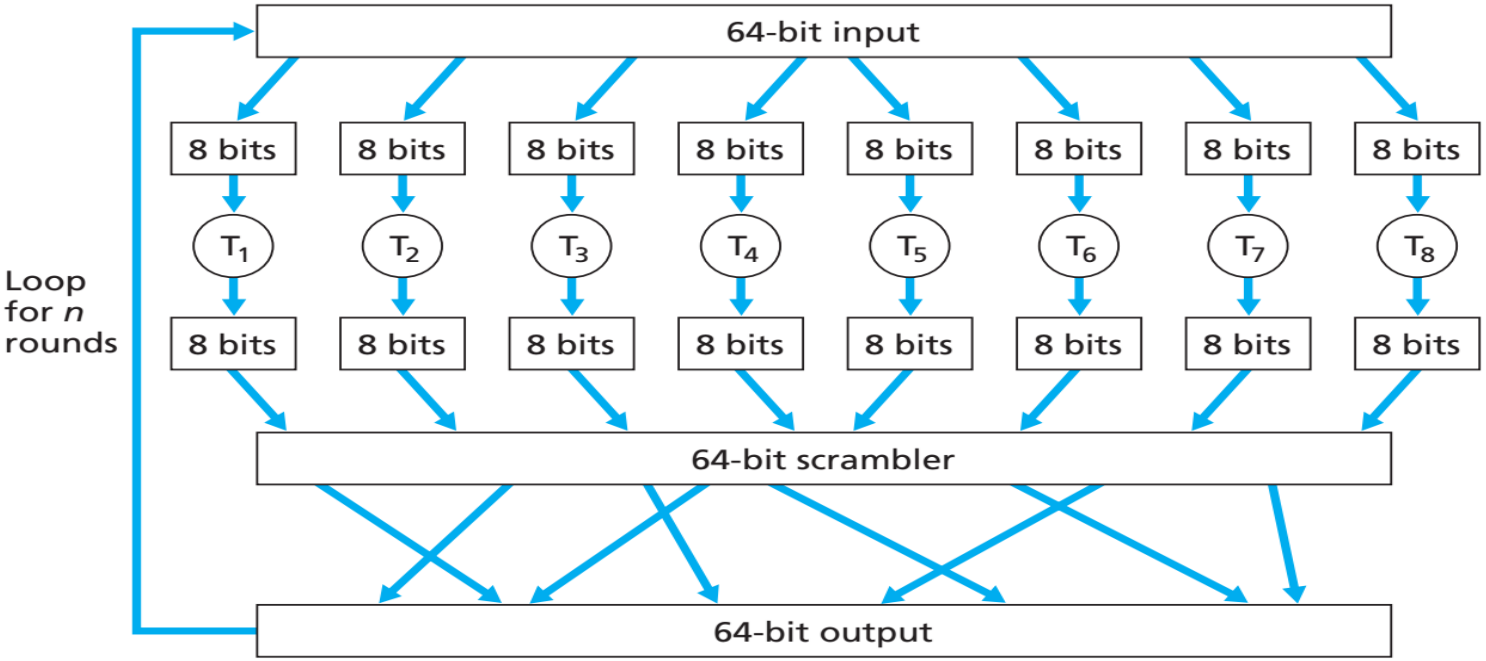
- *Qual o texto cifrado para a mensagem 010110001111?*

RESP: 101000111001

- *Quantas chaves diferentes existem? É fácil quebrar essa criptografia com força bruta?*
- *Um padrão usual hoje é usar k=64. Quantas chaves existem nesse caso? Qual o problema dessa técnica?*

Exemplo 2

- *Diminuindo o tamanho das tabelas: simulando tabelas de permutação aleatórias*



- *Ideia básica para DES, 3DES, AES, etc.*

Criptografia de chave simétrica: DES

DES: Data Encryption Standard

- Padrão de encriptação americano (NIST) até 1976-2001
- Algoritmo de bloco com *encadeamento* (evitar problema de textos abertos iguais gerar textos cifrados iguais fazendo XOR com sequência pseudoaleatória transmitida em aberto)
- chave simétrica de 56 bits para entrada de texto aberto de 64 bits
- Para chave de comprimento *n*, força bruta precisa testar 2^n chaves
- Tornando o DES mais seguro:
  - 3DES: encriptar 3 vezes com 3 chaves diferentes (1998)
- Abandonado em 2001 em favor do AES
- Quão seguro é o DES?
  - Não se conhece bom ataque usando análise estatística
  - Em 2007, máquina paralela de FPGA da Universidade de Bochum e Kiel, Alemanha, viola o DES em aproximadamente seis dias e meio por um custo de $10,000 em *hardware*. *Em 2008, tempo reduzido para menos de um dia.*

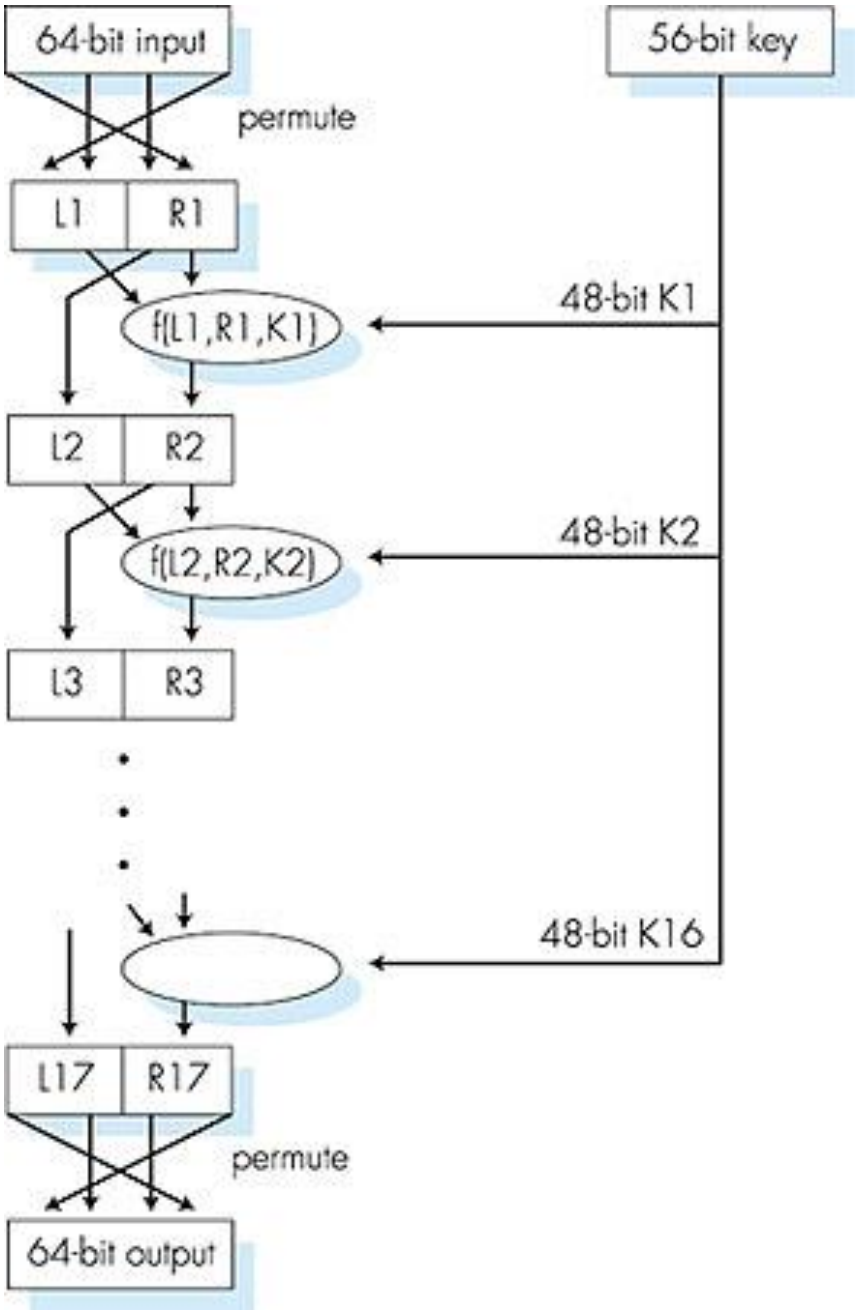
Criptografia de chave simétrica: DES

Operação do DES

permutação inicial

16 "rodadas" idêniticas de aplicação da função, cada uma usando uma chave de 48 bits diferente

permutação final



AES: Advanced Encryption Standard

- Padrão para chave simétrica do NIST, substituiu o DES (Nov 2001)
- Processa dados em blocos de 28 bits
- Chaves com 128, 192, ou 256 bits
- NIST estima que decriptação por força bruta (testar cada chave) levará 149 trilhões de anos para uma máquina que leve 1 s para descriptar DES (mais aqui)
- "De acordo com os documentos divulgados por Snowden, a NSA está pesquisando se ataques criptográficos baseados em *tau statistic* podem ajudar a quebrar o AES."
- "Até o momento, não se conhece nenhum ataque prático que poderia permitir que alguém sem conhecimento da chave ler dados encriptados pelo AES quando ele é corretamente implementado."

AES: Advanced Encryption Standard

- O CAVP (Cryptographic Algorithm Validation Program) do NIST fornece validação independente da correta implementação do algoritmo AES. A validação com sucesso resulta em aparecer na lista *NIST validations*

- Vetores de teste são um conjunto de cifras dada uma entrada e a chave. O NIST distribui vetores de teste referência para o AES: AES Known Answer Test (KAT) Vectors (in ZIP format).

- WhatsApp usa...