Criptografia

- Cripto = oculto/escondido + Grafia = escrita
  - Criptografia = arte de escrever oculto, em código
- Elementos da criptografia
  - Codificação (encriptação)
    - embaralhamento de um conteúdo de forma que fique ininteligível a quem não possui a "chave" para restaurar
  - Cripto-Algoritimo, Criptosistema ou Cifra: método
  - Chave: elemento combinado ao algoritmo para permitir combinações/variações

Mensagem/ Texto-**P**uro → **e**ncriptação → Texto-**C**ifrado → **d**ecriptação → **P**

Criptografia

- Criptografia: grande ferramenta de segurança
  - Elemento básico: Confidencialidade
  - Também pode garantir: Integridade, Autenticação, Controle de acesso, Não-repúdio
- Criptoanálise
  - Estudo de meios p/quebrar códigos de criptografia
  - Toda cifra pode ser quebrada de alguma forma
  - Sucesso do método é a dificuldade de quebrá-lo
- Algoritmo computacionalmente seguro
  - Custo de quebrar excede o valor da informação
  - O tempo para quebrar excede a vida útil da info.

Criptografia

- Meios de criptoanálise
  - Força bruta: tentar todas as possibilidades
  - Mensagem conhecida
  - Mensagem escolhida (conhecida e apropriada)
  - Análise matemática e estatística
  - Engenharia social
- Conceitos para bom algoritmo de criptografia
  - Confusão
    - transformações na cifra de forma irregular e complexa
  - Difusão
    - pequena mudança na mensagem, grande na cifra

Criptografia

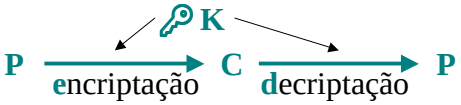
- Categorias de cifra:
  - Seqüencial: em geral mais fraca, baixa difusão
  - Bloco: mais usada
- Exemplos

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
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	A
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

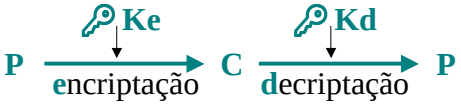
  - EXEMPLIFIQUE
  - EXEMPLIFIQUE ⩾ XEMELPFIQIEU (inverte cada 2 letras)
  - A A A A A A | B A A A A A
    A B C D E F | B C D E F G (deslocamento pela letra ant.)

Criptografia

- Tipos de função de criptografia
  - Chave secreta, Simétrica ou Convencional
    - Existência de uma única chave secreta (K)

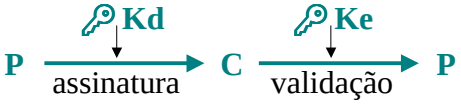


  - Chave pública ou Assimétrica
    - Existência de par de chaves: pública (Ke) e privada (Kd)



Criptografia

- Outras aplicações relacionadas
  - Chave pública como Assinatura digital



  - Autenticação de mensagem
    - Validar a integridade da mensagem (contra falsificação)
    - Existem técnicas criptográficas baseadas em chave (Message Authentication Code - MAC) e outras não criptográficas (algoritmos hash uni-direcionais)

Criptografia Convencional

- Convencional
  - Chave secreta única, compartilhada entre origem e destino
  - Simétrica: decodificação é o inverso da codificação
  - Aplicação principal: **Confidencialidade**, privacidade
- Requisitos
  - Conhecido o algoritmo e texto-cifrado, deve ser difícil decifrar ou obter a chave
  - A chave deve ser compartilhada de forma segura entre remetente (origem) e destino
- Vantagens
  - Rápida
  - Privacidade segura
  - Ampla compreensão
- Desvantagens
  - Chave secreta compartilhada
  - Sem autenticação única
  - Sem não-repúdio

Criptografia Convencional

- Principais algoritmos
  - Data Encryption Standard/Algorithm (DES/DEA)
    - Mais conhecido, inventado pela IBM em 1971
    - Evolução: Triplo DES (3DES, TDES ou TDEA)
  - International Data Encryption Standard (IDEA)
    - Instituto Federal de Tecnologia da Suíça, 1991
  - Blowfish
    - Bruce Schneier, 1993
  - RC5
    - Ron Rivest (RSA Laboratories), 1994
  - CAST
    - Carlisle Adams & Stafford Tavares, 1997
- Futuro (padrão a ser adotado pelo NIST):
  - Advanced Encryption Standard (AES)

Criptografia Convencional

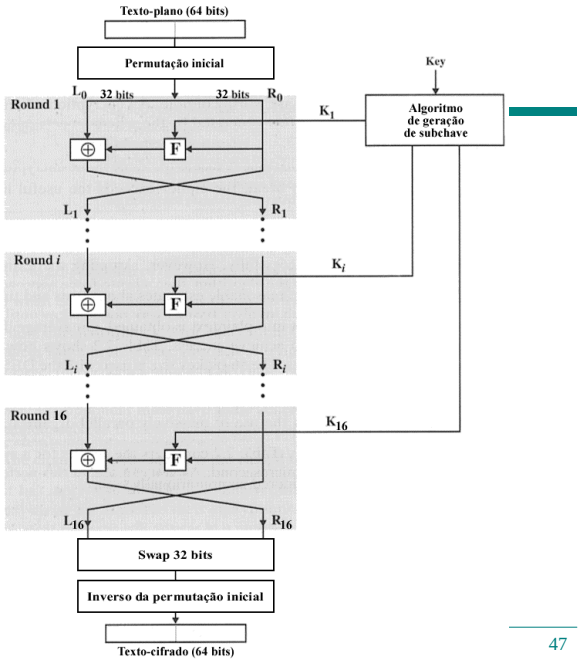
- Comparativo de algoritmos

Algorithm	Key Size	Number of Rounds	Mathematical Operations	Applications
DES	56 bits	16	XOR, fixed S-boxes	SET, Kerberos
Triple DES	112 or 168 bits	48	XOR, fixed S-boxes	Financial key management, PGP, S/MIME
IDEA	128 bits	8	XOR, addition, multiplication	PGP
Blowfish	Variable to 448 bits	16	XOR, variable S-boxes,addition	
RC5	Variable to 2048 bits	Variable to 255	Addition, subtraction, XOR, rotation	
CAST-128	40 to 128 bits	16	Addition, subtraction, XOR, rotation, fixed S-boxes	PGP

Criptografia Convencional

- DES
  - O algoritmo de criptografia convencional mais usado é o DES (Data Encryption Standard) ou DEA (Data Encryption Algorithm)
  - O DES foi inventado pela IBM em 1971
  - Foi adotado em 1977 pelo NIST (National Institute of Standards and Technology, EUA)
  - Era essencial a implementação em hardware
  - O DES criptografa blocos de 64 bits usando uma chave de 56 bits
  - O DES executa 16 "rodadas" de criptografia

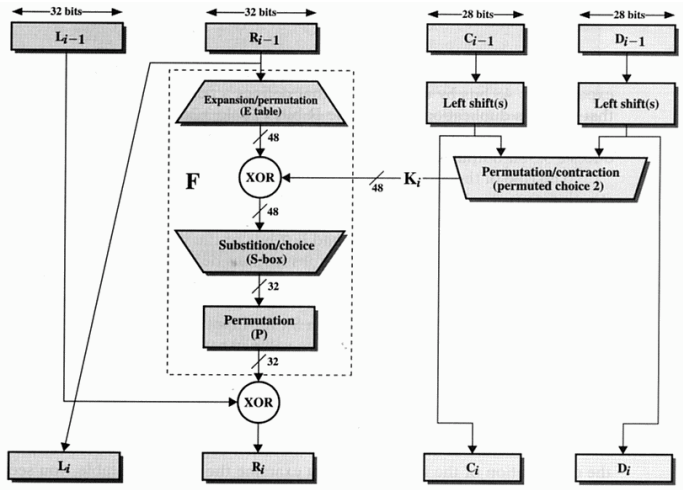
DES



Algoritmo do DES

- Rodada do DES
  - Cada rodada usa uma sub-chave gerada a partir da chave original
  - As operações matemáticas em cada rodada são as mesmas
  - A diferença está na sub-chave e na função *F*
  - As funções de expansão, contração e permutação de bits são diferentes para cada rodada
  - O objetivo dos S-box e das permutações é quebrar a linearidade dos dados
  - A conseqüência é a dificuldade da inversão da operação de criptografia

Rodada do DES



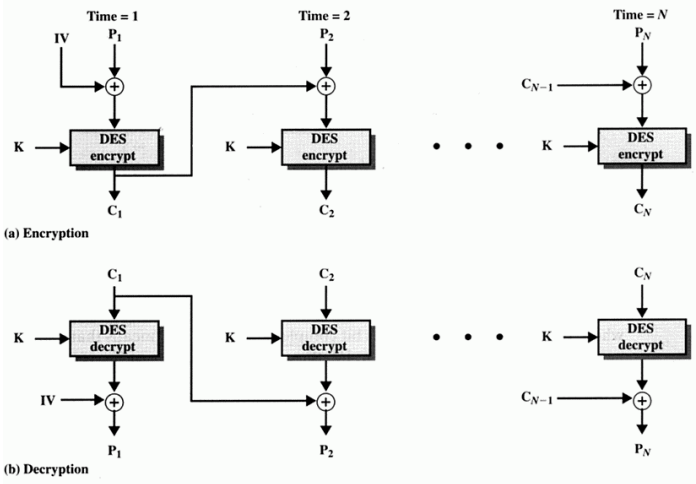
Segurança do DES

- Existem 2^{56} chaves possíveis de 56 bits (~ $7{,}2 \times 10^{16}$)
- Em 1993 foi feito um estudo de custo de uma máquina paralela para quebrar o DES:

Key Search Machine Unit Cost	Expected Search Time
$100,000	35 hours
$1,000,000	3.5 hours
$10,000,000	21 minutes

- Desafio
  - Em 29 de janeiro de 1997, RSA Laboratories publicou um desafio de quebrar uma mensagem cifrada com DES
  - Um consultor desenvolveu um programa de força bruta e o distribuiu pela Internet
  - 96 dias depois a mensagem foi quebrada
  - Mais de 70.000 máquinas foram usadas

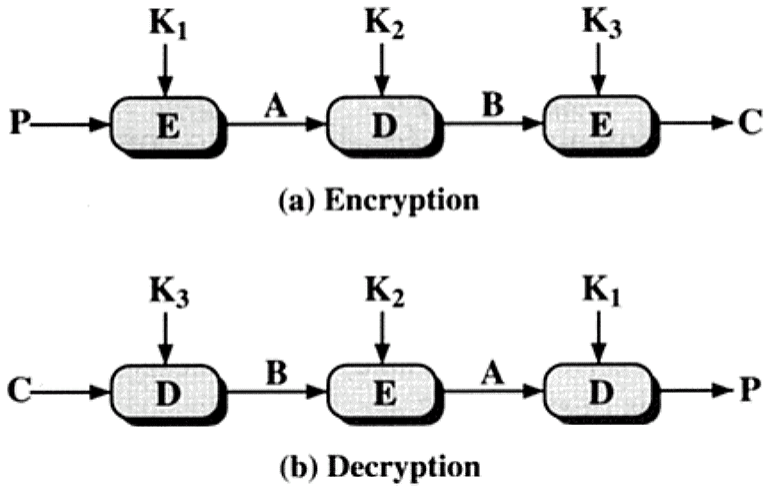
Encadeamento de DES



Triplo DES (3DES)

- Para melhorar a segurança do DES, o algoritmo pode ser aplicado mais vezes em seqüência
- A forma mais simples é usar o DES 2 vezes
- Porém, dadas as chaves K1 e K2, é possível encontrar K3 tal que $E_{K2}[E_{K1} [P]] = E_{K3} [P]$
- Portanto, a forma mais comum de aplicar o DES mais vezes é em seqüências de 3
- 3DES comumente usa uma seqüência E-D-E

3DES



3DES

- 3DES corresponde, com 3 chaves de 56 bits, a uma chave efetiva de 168 bits

$$C = E_{K1} [D_{K2} [E_{K3} [P]]]$$

- O algoritmo 3DES também pode ser usado com 1 ou 2 chaves distintas
  - Para duas chaves (112 bits):

$$C = E_{K1} [D_{K2} [E_{K1} [P]]]$$

  - Para uma chave (56 bits), se torna o DES comum:

$$C = E_{K1} [D_{K1} [E_{K1} [P]]] = E_{K1} [P]$$

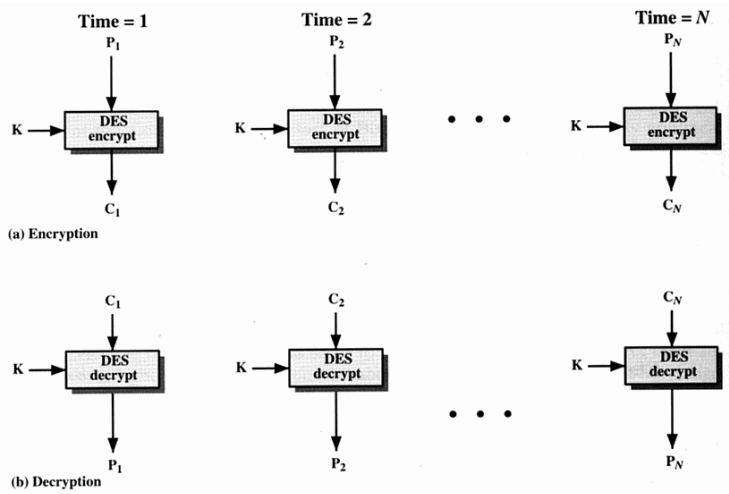
DES – Conclusão

- É eficiente (principalmente em hardware)
- Apesar do DES ser um algoritmo antigo, ganhou sobrevida com o 3DES
- A vantagem é o aproveitamento de todo software e hardware já criado
- 3DES é compatível com o DES usando 1 chave somente

Encadeamento de Blocos

- Os textos em geral "medem" muitos blocos
- Caso do DES: cada bloco 64 bits armazena apenas 8 letras ASCII
- Se a mesma chave for usada para criptografar todos os blocos do texto, surgirão padrões de repetição de blocos (cifras iguais para blocos iguais)
- Quanto maior o texto, maior a quantidade de padrões repetidos para análise
- Electronic codebook (ECB): dada uma chave, o resultado é fixo para cada bloco de texto. Pode-se imaginar um "livro gigante" com cada bloco de texto possível (como um "alfabeto") e a cifra resultante, como uma mera tabela de transposição

Encadeamento de Blocos



Encadeamento de Blocos

- Para evitar a análise de freqüência de blocos, deve ser usada alguma técnica para que blocos iguais gerem cifras diferentes ao longo do texto
- Uma solução é fazer com que as chaves de criptografia dos blocos não sejam as mesmas
- Outra solução é compactar o texto antes da criptografia, o que elimina padrões originais
- A técnica mais comum é o encadeamento de blocos: cada bloco afeta o seguinte

Criptografia Convencional

- **Futuro** NIST: Advanced Encryption Standard (AES)
- Requisitos mínimos definidos para o AES:
  - Algoritmo publicamente definido
  - Ser uma cifra simétrica de bloco
  - Projetado para que o tamanho da chave possa aumentar
  - Implementável tanto em hardware quanto em software
  - Disponibilizado livremente ou em acordo com termos ANSI
- Fatores de julgamento:
  - Segurança (esforço requerido para criptoanálise)
  - Eficiência computacional
  - Requisitos de memória
  - Adequação a hardware e software
  - Simplicidade
  - Flexibilidade
  - Requisitos de licenciamento

Criptografia Convencional

- Seleção do Advanced Encryption Standard (AES)
  - Processo seletivo do algoritmo desde 1997
  - Etapa 1: 15 candidatos selecionados em Agosto 1998
  - Etapa 2: 5 finalistas anunciados em Agosto 1999
  - Escolha do vencedor em Outubro 2000
  - Padronização prevista para 2º semestre 2001
  - Vencedor: **Rijndael** – Vincent Rijmen, Joan Daemen
  - Outros algoritmos finalistas:
    - MARS – IBM
    - RC6 – RSA Laboratories
    - Serpent – Ross Anderson, Eli Biham, Lars Knudsen
    - Twofish – Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Distribuição de Chaves

- A distribuição de chaves é o ponto fraco dos algoritmos de chave secreta