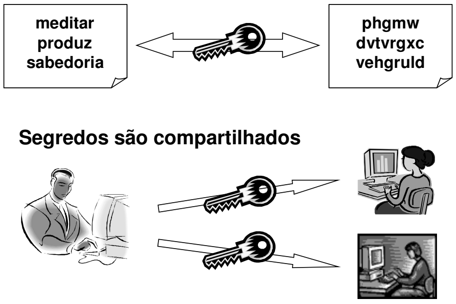
Sistemas criptográficos simétricos



meditar
produz
sabedoria

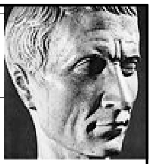
phgmw
dvtvrgxc
vehgruld

Segredos são compartilhados

Criptografia Convencional: Técnicas Clássicas

- **Técnica de substituição**
  - – Letras do texto plano são substituídas por outras letras.
- **Técnica de transposição**
  - – Letras do texto plano são permutadas entre si.

Técnicas de Substituição



- **Cifrador de César**

p:texto plano abcdefghijklmnopqrstuvwxyz
C:texto cifrado DEFGHIJKLMNOPQRSTUVWXYZABC

meditarproduzsabedoria
PHGMWDVTVRGXCVDEHGRULD

cifrar	**decifrar**
C = E(p) = (p+3) mod 26	**p = D(p) = (C-k) mod 26**
C = E(p) = (p+k) mod 26	

Técnicas de Substituição

Cifrador de Vigenère

	a	b	c	..	z
A	A	B	C		Z
B	B	C	D		A
C	C	D	E		B
:					
Z	Z	A	B		Y

k: *proverbioproverbioprove*
p: meditarproduzsabedoria
C: BVRDXRSXFTGHJNDFESIKHUJ

k: *proverbio*meditarproduz
p: meditarproduzsabedoria

Técnicas de Transposição

- Sem uso de chave

m		d		t		r		r		d		z		a		e		o		i	
	e		i		a		p		o		u		s		b		d		r		a

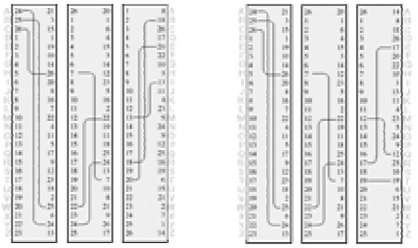
M DTR R D Z A E O I E I A P O U S B D R A

- Com uso de chave

4	6	1	3	2	5
m	e	d	i	t	a
r	p	r	o	d	u
z	s	a	b	e	d
o	r	i	a	x	y

DRAITDEXIOBAMRZOAUDYEPSR

Máquina de Rotores



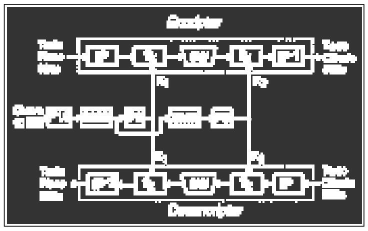
3 rotores **17.576** (26x26x26) alfabetos diferentes,
4 rotores **456.976**,
5 rotores **11.881.376**, ...

Criptografia Convencional: Técnicas Modernas

- **Cifradores de Fluxo**
  - atuam sobre um bit, ou byte, de cada vez.
- **Cifradores de Bloco**
  - atuam sobre um bloco do texto plano, produzindo um bloco de texto cifrado do mesmo tamanho.
- **DES** (*Data Encryption Standard*)
  - opera sobre blocos de 64-bits.

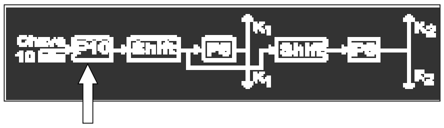
DES Simplificado

Idealizado por Edward Shaefer (Univ. Santa Clara)



IP - permutação Inicial
f_k - função complexa
SW - permutação simples

Geração de Chave no S-DES

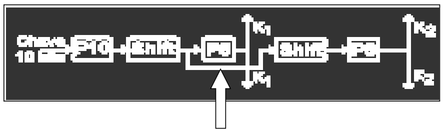


1. Permutação sobre a Chave

- P10 ($k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10}$) = ($k_3 k_5 k_2 k_7 k_4 k_{10} k_1 k_9 k_8 k_6$)
- Assim: Chave 1010000010
  Permutação Inicial 1000001100

A chave K (10-bits) produz duas chaves: K_1 e K_2 de 8-bits cada

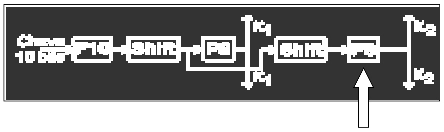
Geração de Chave no S-DES



2. Produção K1

– Separação de P10	10000 01100
– Rotação a esquerda LS-1	00001 11000
– Aplicação da tabela P8	(k_6 k_3 k_7 k_4 k_8 k_5 k_{10} k_9)
– Resultado é a sub-chave K1	10100100

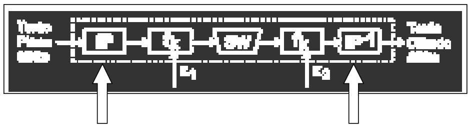
Geração de Chave no S-DES



3. Produção K2

– Resultado de LS-1	00001 11000
– Rotação a esquerda LS-2	00100 00011
– Aplicação da tabela P8	(k_6 k_3 k_7 k_4 k_8 k_5 k_{10} k_9)
– Resultado é a sub-chave K2	01000011

Encriptação no S-DES

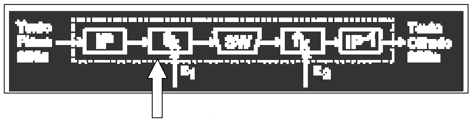


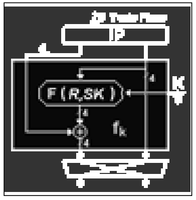
- **IP** = 2 6 3 1 4 8 5 7 **IP^{-1}** = 4 1 3 5 7 2 8 6

Exemplo: 11110011 **IP** = 10111101
IP^{-1} = 11110011

- **IP^{-1}** (**IP** (X)) = X

Encriptação no S-DES



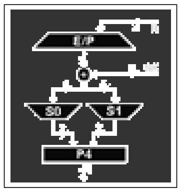


- f_k : combinação das funções de permutação e substituição
- f_k (*L, R*) = (*L* ⊕ F (*R, SK*), *R*)

- *L e R* = 4-bits à esquerda e 4-bits à direita
- ⊕ = ou exclusivo
- **F** = função de mapeamento sobre ***R e***
- a sub-chave ***SK***

Encriptação no S-DES

- **F (** ***R, SK*** **)** = Função de mapeamento sobre R e a sub-chave SK



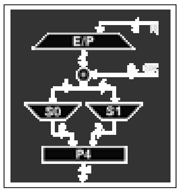
- E/P = Expansão / Permutação
- = 4 1 2 3 2 3 4 1

ex : 1101 → 11101011

- ⊕ = OU exclusivo com a chave SK
- ex : 11101011 ⊕ 01000011
- 10101000

Encriptação no S-DES

- **F (** ***R, SK*** **)** = Função de mapeamento sobre R e a sub-chave SK

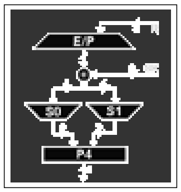


$$S0 = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{pmatrix} \qquad S1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

Em S0 e S1, linha = 1° e 4° bits
coluna = 2° e 3° bits
ex: 1010 1000 S0 = 2 → 10
S1 = 3 → 11

Encriptação no S-DES

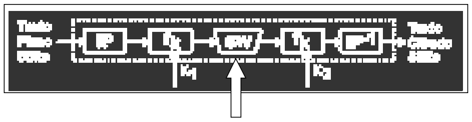
- **F (** ***R, SK*** **)** = Função de mapeamento sobre R e a sub-chave SK



Em P4 as saídas de S0 e S1 são concatenados e permutação sendo a tabela:
P4 = 2 4 3 1

ex: 10 11 → 0111

Encriptação no S-DES



SW : executa uma simples troca entre os 4-bits da direita com os 4-bits da esquerda

ex: 0111 sw 0100 → 01000111

- Resultado de Sw é utilizado como entrada para uma nova aplicação da função f_k, utilizando desta vez a chave K_2.

Desencriptação no S-DES

DES (*Data Encryption Standard*)

- Definido como:

$$IP^{-1} \circ f_{k16} \circ SW \circ f_{k15} \circ SW \circ \ldots \circ f_{k1} \circ IP$$

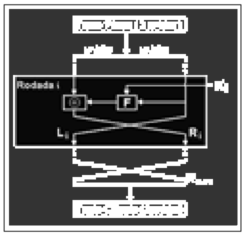
  - opera sobre blocos de 64-bits
  - chaves de 56-bits
  - função F atua sobre 32-bits
  - 8 caixas de 16 colunas

Cifrador de Feistel

Feistel propôs a troca de uma simples substituição pela utilização de um cifrador de produto, o que seria análogo ao uso alternado entre substituição e permutação.

- Cifrador produto alterna:
  - *confusão*, técnica de criptografia que leva em conta a relação entre as estatísticas do texto cifrado e o valor da chave de encriptação.
  - *difusão,* é técnica de criptografia que busca obscurecer a estrutura estatística do texto, distribuindo a influência de cada digito sobre o texto cifrado

Cifrador de Feistel

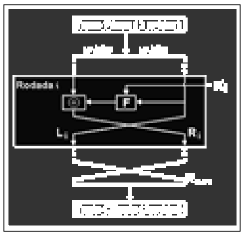


Entrada: texto plano de 2 w bits,
e a chave *K.*

Rodadas:
⊕: substitiução
F: função parametrizada pela chave

Saída: texto cifrado de 2 w bits

Cifrador de Feistel



- Características:
- Tamanho do bloco, 64-bits
- Tamanho da chave, 128-bits
- Número de rodadas, 16 padrão
- Algoritmo de geração sub-chaves
- Função ciclo (F)
- Eficiência do algoritmo
- Facilidade de análise