Cifra de Bloco
AES – *Advanced Encryption Standard*

Prof. Dr. Avelino Francisco Zorzo
Faculdade de Informática – PUCRS

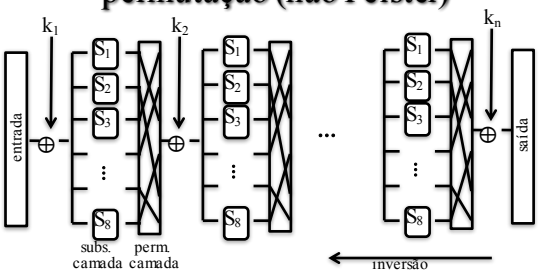
Advance Encryption Standard

- 1997: NIST publicou chamada para propostas
  - Requer blocos de 128 bits e suporte para chaves de 128, 192 e 256 bits
- 1998: 15 submissões
- 1999: NIST escolheu 5 finalistas
  - MARS, RC6, Rijndael, Serpent and Twofish
- 2000: NIST escolheu Rijndael como AES
  - Projetado por Rijmen e Daemen

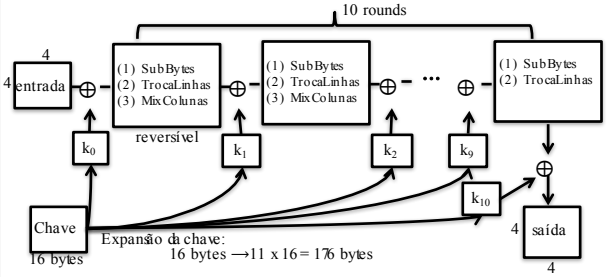
Sumário dos 5 finalistas

Nome	Autor	Tipo
Mars	IBM	Rede de Feistel Extendida
RC6	RSA	Rede de Feistel
Rijndael	Joan Daemen e Vincent Rjimen	Rede de Substituição e Permutação
Serpent	Ross Anderson, Eli Biham, e Lars Knudsen	Rede de Substituição e Permutação
Twofish	Bruce Schneier, John Kelsey, Niels Ferguson, Doug Whiting, David Wagner e Chirs Hall	Rede de Feistel

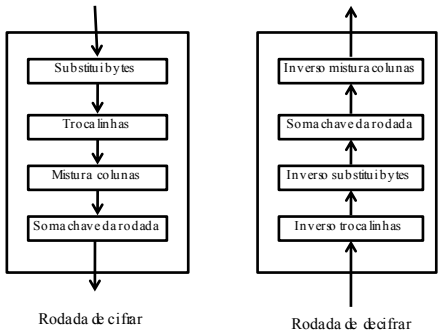
AES é uma rede de substituição e permutação (não Feistel)



Esquemático (AES-128)



AES Cifrar/Decifrar



SubBytes

Cifra de substituição (26 letras)

A	A
B	B
C	C
D	D
E	E
…	…
Y	Y
Z	Z

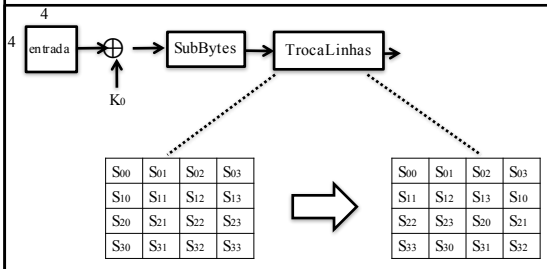
SubBytes no AES (entrada de 8 bits)

00000000	00000000
00000001	00000001
00000010	00000010
00000011	00000011
00000100	00000100
…	…
11111110	11111110
11111111	11111111

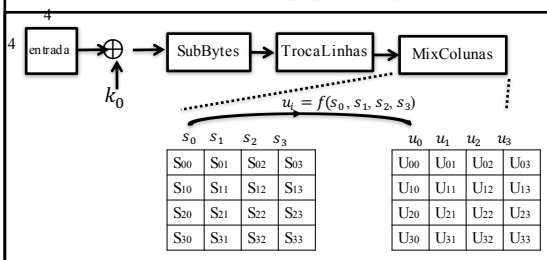
Resumo: SubBytes

- Diferente do DES, as caixas S não são aleatórias
  - Está definido na teoria dos corpos
- Diferente do DES, as caixas S não precisam ser inseridas no códigos (*hard-coded*)
  - Permite uma codificação pequena (por exemplo em *smartcards*)
- Balanço flexível entre tamanho e desempenho

Troca Linhas



MixColunas



- Cada byte em uma coluna é trocado por duas vezes aquele byte, mais três vezes o próximo byte, mais o byte que vem depois, mais o byte que vem depois.
  - Exemplo: $U_{00} = 2xS_{00}+3xS_{10}+S_{20}+S_{30}$

Escalonamento da chave (AES-128)

- Expandir 16 bytes (onze vezes) em 176 bytes
- AES define uma palavra que consiste de 4 bytes

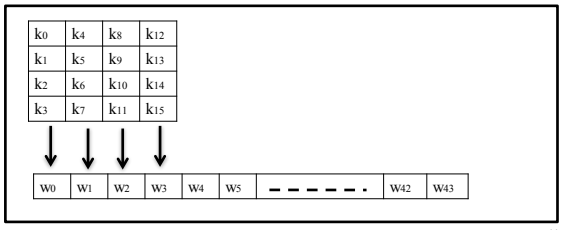
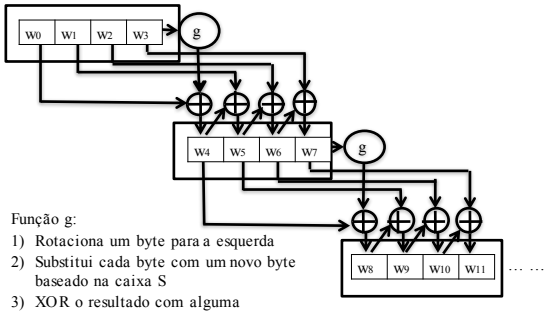


Diagrama do escalonamento



Função g:

1) Rotaciona um byte para a esquerda
2) Substitui cada byte com um novo byte baseado na caixa S
3) XOR o resultado com alguma constante

Variantes do AES

- Os blocos são sempre de 128 bits
- As chaves são diferentes: 128, 192, 256
  - AES-128: 10 rodadas
  - AES-192: 12 rodadas
  - AES-256: 14 rodadas
- Os algoritmos de escalonamento das chaves são diferentes