UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança da Informação
Aula 6 – Principais Algoritmos Simétricos. Criptografia Assimétrica.

Prof. Dr. Eng. Fred Sauer

fsauer@gmail.com

http://www.fredsauer.com.br

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Algoritmos

- Alguns cifradores simétricos:
  - DES, 3DES
  - RIJNDAEL (AES)
  - BLOWFISH
  - RC2
  - RC4 → Único de Fluxo
  - IDEA
  - RC5
  - TWOFISH
  - SERPENT

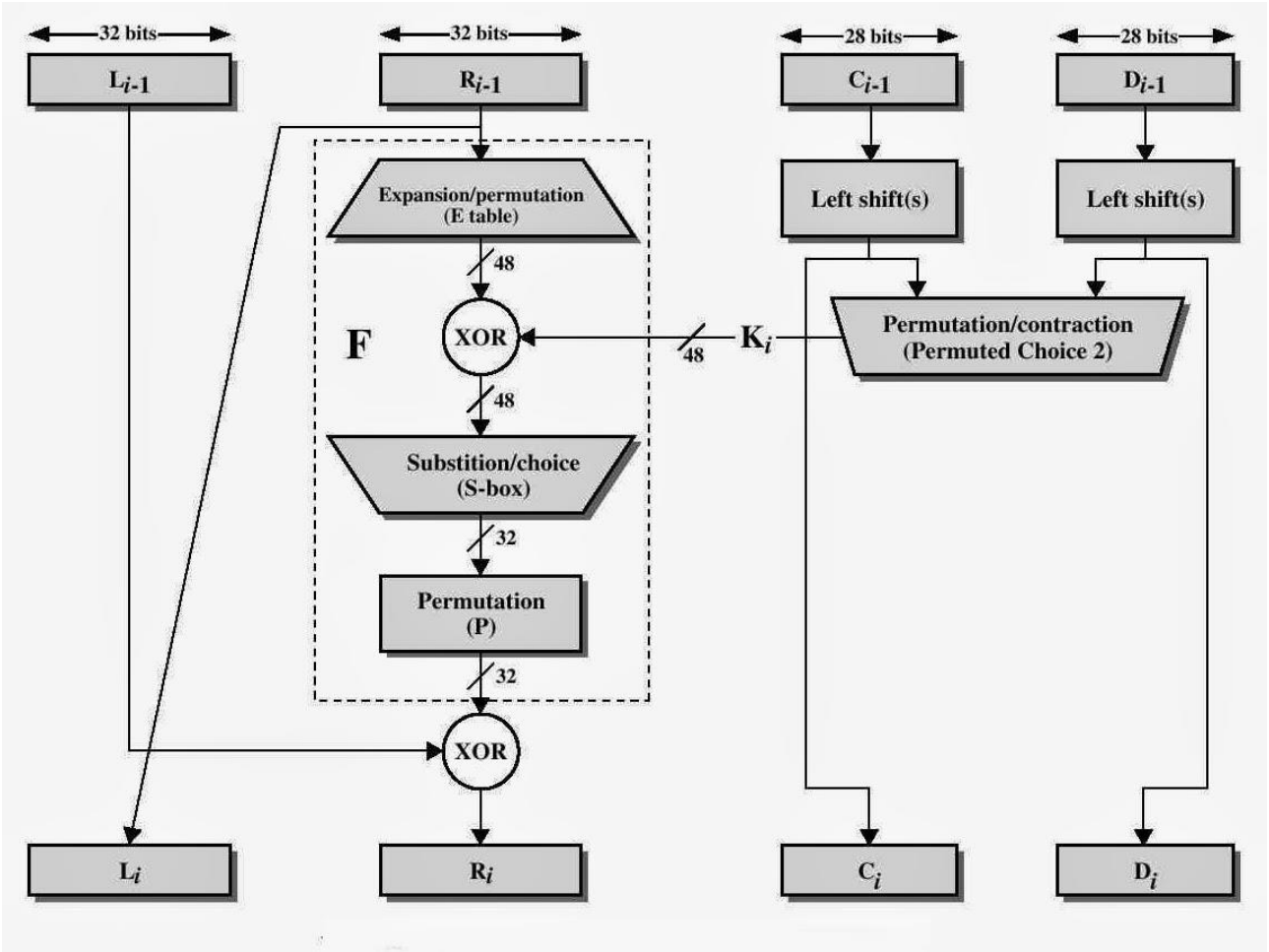
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

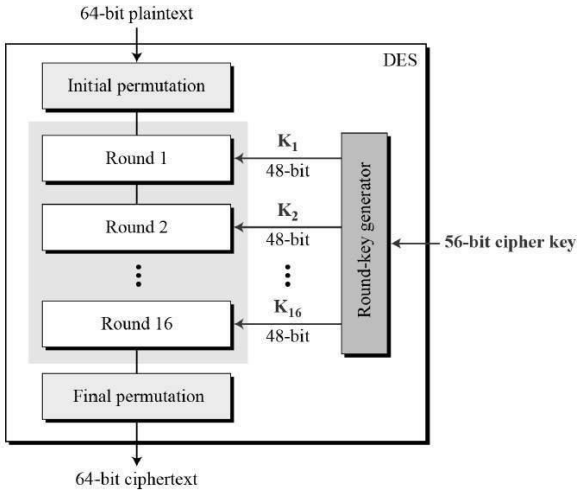
Criptografia
DES (Data Encryption Standard)

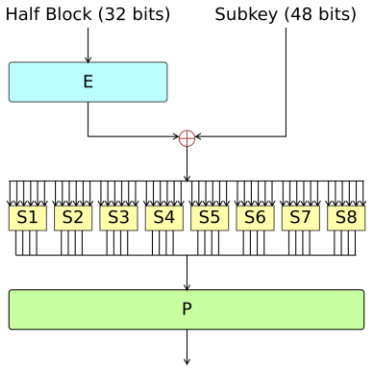
- Cifrador mais conhecido do mundo
- Originado a partir do LUCIFER (IBM - Feistel)
- Aprovado como padrão em 1977
- Mensagem: 64 bits
- Chave: 64 bits = 56 utilizados + 8 paridade
- Mensagem cifrada: 64 bits

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
DES(Data Encryption Standard)

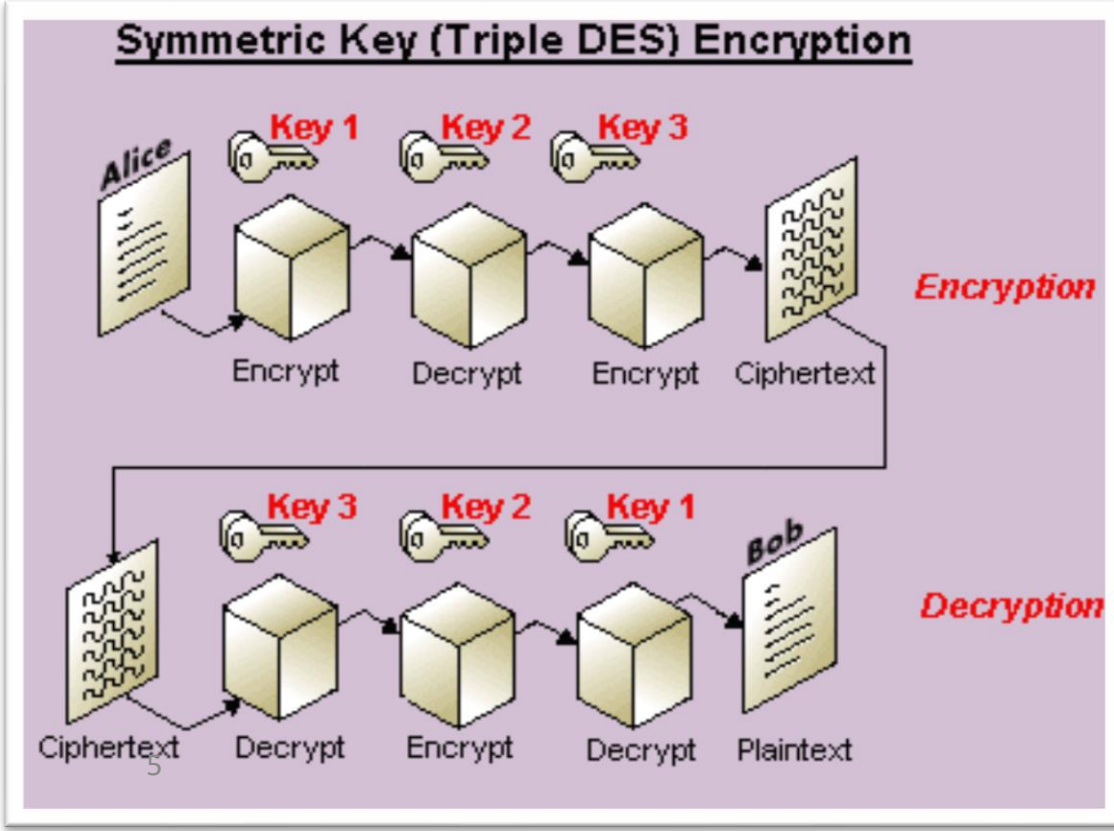






Criptografia
3DES(Triple Data Encryption Standard)

- Criptografa 3 vezes com 3 chaves diferentes
  (na verdade, criptografa, decriptografa, criptografa)
- Chave: 168 bits



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
RIJNDAEL (AES)

- Projetista: Vincent Rijmen e Joan Daemen.
- Janeiro de 1997, origem AES
- **NIST (National Institute of Standards and Technology)**, órgão do Departamento de Comércio dos EUA, encarregado de aprovar padrões para o governo federal dos EUA patrocinou um **concurso** para um novo padrão criptográfico para uso não-confidencial
- A transparência da seleção gerou confiança do público no algoritmo.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
RIJNDAEL (AES)

- Tamanho da chave: 128 a 256 bits
- Comentário:
  - Muito forte
  - Atual AES
- Para fins comerciais, a chave de 128 bits já oferece segurança extremamente elevada:
  - 128 bits → 2^{128} combinações.
  - Para "quebrar por força bruta":
    - Máquina com 1 bilhão de processadores paralelos.
    - Cada um realizando um teste a cada pico segundo → 1 trilhão/segundo.
    - 10.000.000.000 de anos para testar todas as combinações.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Resumo Algoritmos Simétricos

Algoritmo	Tamanho chave
DES	56 bits
3DES	112 ou 168 bits
Blowfish	1-448 bits
RC2	1-2048 bits
RC4	1-2048 bits
IDEA	128 bits
RC5	128-256 bits
Twofish	128-256 bits
Serpent	128-256 bits
Rijndael	128-256 bits

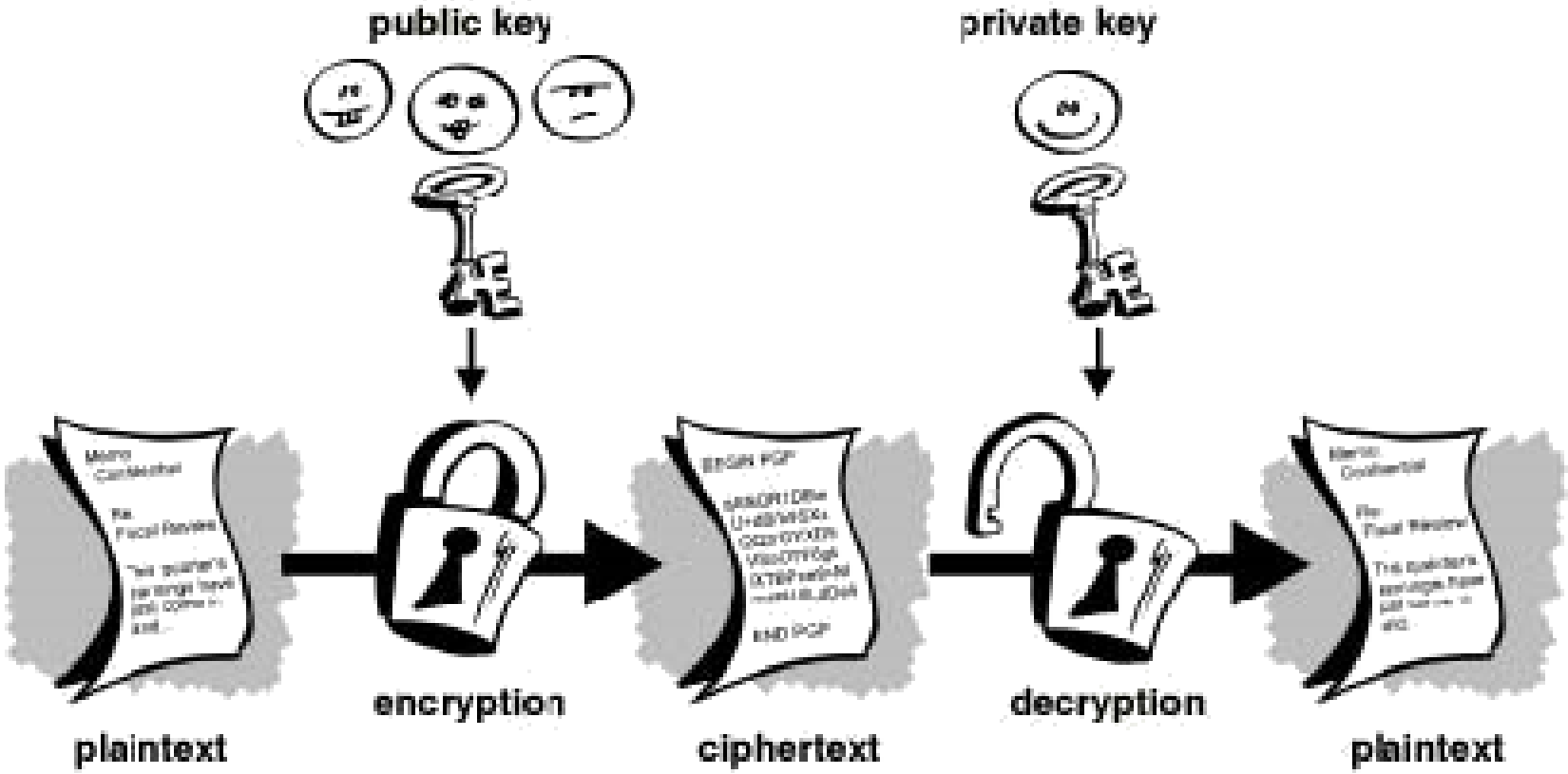
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Criptografia Simétrica

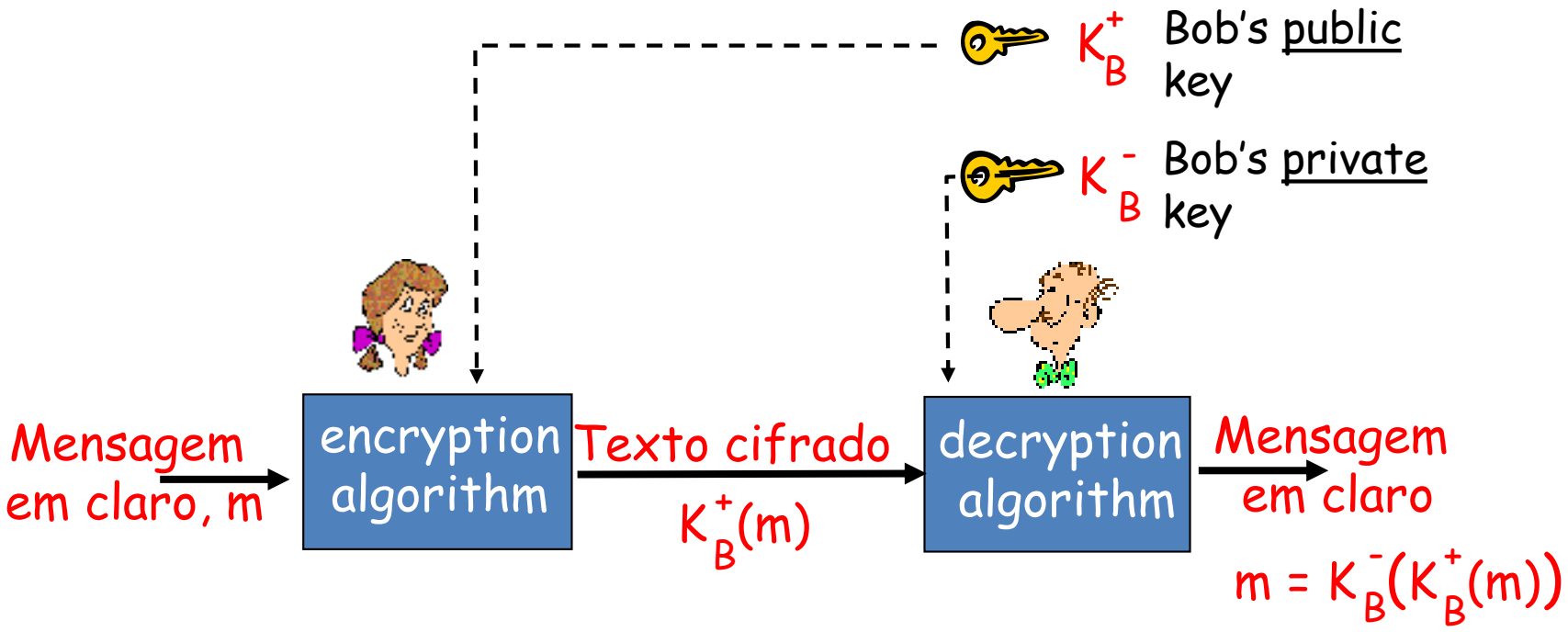
- Chave simétrica
  - A chave deve ser protegida. Se um terceiro descobrir a chave poderá:
    - Interceptar a comunicação
    - Alterar/forjar mensagens
  - Problemas:
    - Como transmitir a mensagem para o receptor com segurança?
    - Como o emissor/receptor pode garantir que a mensagem não foi alterada?
    - Como o receptor pode ter a garantia de que a mensagem foi realmente enviada pelo emissor declarado?

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Criptografia Assimétrica



Criptografia com chave pública (assimétrica)



Obs: $m = K_B^-(K_B^+(m))$ e $m = K_B^+(K_B^-(m))$

Algoritmo RSA: Rivest, Shamir, Adleman algorithm

Criptografia com chave pública (assimétrica)

- No exemplo anterior estabeleceu-se uma comunicação unidirecional de Bob para Alice.
- Alice não precisou se cercar de cuidados ao enviar sua chave a Bob. Como essa chave só permite codificar uma mensagem, ninguém poderia interceptá-la.
- Apenas a chave de decodificação pode reverter o processo e obter a mensagem original.
- Por isso, a chave privada deve ser guardada com extremo cuidado por Alice.

Criptografia com chave pública (assimétrica)

- A chave de codificação de Alice pode ser distribuída livremente, enviada por meios não seguros e até publicada em seu *website*.
  - **CHAVE PÚBLICA**

- A chave de decodificação deve ser guardada por Alice e somente ela deve possuí-la.
  - **CHAVE PRIVADA**

Algoritmo de criptografia de chave pública: propriedade importante

A propriedade a seguir será *muito* útil adiante:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{use chave pública primeiro, seguida por chave privada}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{use chave privada primeiro, seguida por chave pública}}$$

O resultado é o mesmo!

Criptografia
Algoritmos de chave pública/privada

- Proposto por W. Diffie e M. Hellman(1976)
- Baseia-se num par de chaves que permitem uma combinação segura de um segredo (chave simétrica)
- Mais lento que algoritmos de chave simétrica

Alice e Bob escolhem e trocam 2 nºs primos grandes, p e g

Alice escolhe um nº randômico grande, x, e calcula A = p^x mod g

Alice mantém x privado e envia A para Bob

Bob faz o mesmo com y, calculando B e enviando para Alice. B = p^y mod g

A chave K = A^y mod p = B^x mod p

Alice		Bob
p, g		
x		
A		
		y
		B
p=11, g=7		
x=3		
A = 7^3 mod 11 = 2 **A=2**		
		y=6
		B = 7^6 mod 11 = 4 **B=4**
K = 4^3mod 11 = 9		K=2^6 mod 11 = 9

Exemplo:

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
RSA (Rivest-Shamir-Adleman)

- Primeiro algoritmo assimétrico completo (1978)
  - Troca segura de chaves
  - Autenticação de mensagens
  - Não é viável para criptografia de fluxo
- Algoritmo de chave pública mais utilizado
- Provê confidencialidade e assinatura digital
- Segurança: Fatoração de Números Grandes

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Comparativo entre Algoritmos

	Criptografia Simétrica	Criptografia Assimétrica
Velocidade	Alta	Baixa
Confiabilidade	Boa	Muito Boa
Nível de Segurança	Alto	Alto
Requer uma terceira parte confiável	Algumas vezes	Sempre
Quantidade de chaves usadas	Uma	Duas

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia Híbrida

- A criptografia assimétrica exige muito mais processamento em relação à criptografia simétrica → Ordem de 100 vezes.

  - Uma saída para não sobrecarregar o processamento:
    1. Estabelece-se um canal com criptografia assimétrica.
    2. Por este canal, as partes combinam usar um algoritmo de criptografia simétrica e uma chave simétrica.
    3. Inicia-se o novo canal com criptografia simétrica, usando-se a chave combinada anteriormente. Por esse canal será feita a comunicação.
    4. O canal com criptografia assimétrica é encerrado.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia Híbrida

- Híbrida
  - "Meio termo" entre as criptografias
  - Aproveita o que tem de bom das duas partes.
  - Processo que utiliza a criptografia simétrica para o envio/recebimento de mensagens e a criptografia assimétrica no compartilhamento das chaves secretas
- Chave de sessão, K_S
  - Bob e Alice usam RSA ou DHE para combinar uma chave simétrica K_S
  - Quando ambos tiverem K_S, eles usam a criptografia de chave simétrica

Criptografia Híbrida

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Fixação

- Durante muito tempo a referência para a criptografia simétrica era o _____, que foi vencido pelo aumento do poder dos processadores, já que a sua chave era fixa, de _____ bits. O bloco era de _____, porque se somavam mais 8 bits de paridade à chave. Esse algoritmo foi substituído pelo _____, que usa chaves de _____, _____ ou _____, mesmo tamanhos de seus blocos, respectivamente.

DES
56
64
AES
128
192
256

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Fixação

- A criptografia assimétrica não substitui a simétrica, porque ela é muito LENTA, devido ao uso de exponenciações e outras funções matemáticas. Assim, hoje todas as soluções são HÍBRIDAS, porque usam a criptografia simétrica para CRIPTOGRAFAR e a assimétrica para TROCA DE CHAVES e AUTENTICAR.
- O RSA, El Gamal e Diffie-Hellmann são exemplos de algoritmos ASSIMÉTRICOS, enquanto o Blowfish, RC4 e Serpent são SIMÉTRICOS.