Engenharia de Segurança

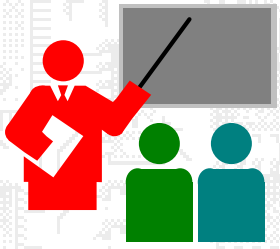
Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco
kalinka@icmc.usp.br

Slides baseados nas transparências de diversos professores e autores de livros (prof. Edward David Moreno, Márcio H. C. d'Ávila, Tannenbaum, Kurose, Adriano Cansian entre outros)

Agenda - Criptografia

1. Serviços Criptográficos
2. Criptografia: Clássica e Moderna
3. Principais Algoritmos Simétricos

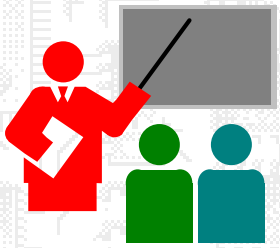
11/22/2010



2

III. CRIPTOGRAFIA CONVENCIONAL

Técnicas Modernas



3

Algoritmo DES

- DES - "*Data Encryption Standard*"
- **Antigo padrão** para uso no governo federal dos EUA
- Padrão definido pelo NIST (*National Institute of Standards and Technologies*)

4

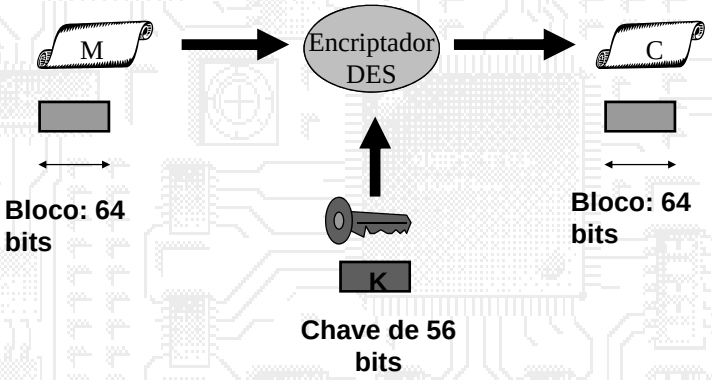
Algoritmo DES - Histórico

- 1977: Adotado como padrão para o governo federal (EUA), exceto para informações secretas/militares
- 1994: NIST reafirma a utilização do DES para uso federal nos EUA por mais 5 anos (até 1999)
- 1997: NIST requisita propostas para um novo algoritmo:
  - AES: Advanced Encryption Standard
  - www.nist.gov/aes

5

Algortimos DES - Encriptação

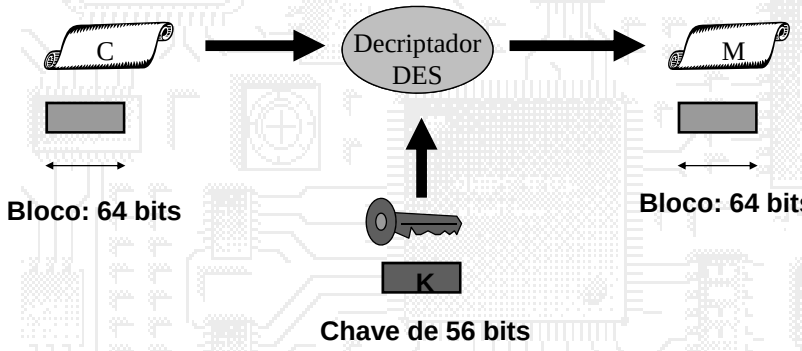
- Encriptação



6

Algortimos DES - Decriptação

- Decriptação



7

Algortimos DES - Problemas

- Problemas
  - Atualmente é considerado um algoritmo **extremamente inseguro**, principalmente para **atividades financeiras**

A Força do DES

Custo da Máquina	Tempo de Busca
$100.000	36 minutos
$1.000.000	3,5 minutos
$10.000.000	21 segundos

8

CUSTOS - DES

- Custo de Decodificação
  - 486 a 66 MHz pode encriptar 344 Kbytes/s
  - Chip VLSI específico para DES pode encriptar 64 Mbytes/s

9

CRÍTICAS AO DES

- Padronização de um algoritmo de criptografia
  - Padrão para uso federal EUA, exceto para informações secretas/militares
  - Largamente utilizado motivado principalmente pela padronização
  - A padronização deixa o algoritmo especialmente vulnerável já que torna o desenvolvimento de técnicas de criptoanálise atraente pois permite sua utilização em diversos segmentos
    - **Viabiliza a construção de uma máquina específica**

10

CRÍTICAS AO DES

- Número de bits (do bloco e da chave) reduzido:
  - É a principal crítica ao algoritmo
  - Redução ocorreu no número de bits do bloco e da chave
  - Com uma chave de comprimento de 56 bits existem 2^{56} possíveis chaves (aprox. $7{,}2 \times 10^{16}$)
  - Utilizando força bruta e realizando 1 encriptação por us (1973), levaria 1.142 anos.
  - Atualmente é relativamente fácil de quebrar.

11

CRÍTICAS AO DES

- Redução do Número de bits (continuação)
  - Em 1977 foi mostrada a possibilidade de construção de uma máquina específica.
    - Custo: US 20 milhões
    - 1 milhão encriptações/us
    - Demoraria 10 horas para a "quebra"
  - Em 1993 (Michael Wienner) foi mostrado que era possível construir uma máquina que utilizava ataque "plaintext Conhecido" que demoraria:
    - 35 horas : Custo de US 100 mil
    - 3,5 horas : Custo de US 1 milhão
    - 21 minutos : Custo de US 10 milhões
  - Provavelmente agências de inteligência dos governos possui este hardware.

12

CRÍTICAS AO DES

- S-BOX
  - Existem módulos internos chamados de S-BOX que podem ter sido definidos (pelo NIST e IBM) utilizando um determinado algoritmo
  - Se isto realmente ocorreu, facilitaria a criptoanálise.
- Serviços de Inteligência dos EUA
  - A definição de um padrão evitaria o surgimento de vários algoritmos de criptografia, facilitando o trabalho das agências de inteligência

13

MODOS DE OPERAÇÃO DO DES

- ECB: Eletronic CodeBook Mode
- CBC: Cipher Block Chaining Mode
- CFB: Cipher FeedBack Mode
- OFB: Output FeedBack Mode

14

MODOS DE OPERAÇÃO DO DES

- ECB: Eletronic CodeBook Mode
  - É o modo mais simples de operação
  - Encriptação por bloco de 64 bits
  - Cada bloco é encriptado de forma independente utilizando uma mesma chave
  - O termo codebook é usado porque, dada uma chave existe um único ciphertext para cada bloco de 64 bits de plaintext.

15

MODOS DE OPERAÇÃO DO DES

- ECB: Características
  - Ideal para mensagens pequenas
  - Inseguro para mensagens grandes
- ECB: Problemas
  - Um mesmo bloco (64 bits) sempre é codificado da mesma forma.

16

MODOS DE OPERAÇÃO DO DES

- CBC: Cipher Block Chaining Mode
  - Permite que um mesmo bloco de plaintext (64 bits) produza encriptações diferentes.
  - Cada bloco a ser cifrado é alterado em função da cifragem anterior
    - Como na primeira iteração, não existe encriptação anterior, uma sequência de 64 bits (Vetor Inicial) é utilizado)
    - o VI (Vetor Inicial) deve ser conhecido tanto por ambas as partes, asssim como a chave.
  - Características:
    - Pode ser utilizado na criptografia de mensagens grandes
    - Pode ser utilizado para autenticação.

17

MODOS DE OPERAÇÃO DO DES

- CFB: Cipher FeedBack Mode
  - Permite utilização em sistemas onde o bloco básico não seja de 64 bits.
  - Permite operação on-line, ou seja, se um bloco básico precisa ser transmitido ele pode ser imediatamente codificado e transmitido.
  - Aplicação distribuída: duas entidades A e B
  - Unidade básica da informação trocada é o byte. Ex. Acontece no TELNET.

18

MODOS DE OPERAÇÃO DO DES

- CFB: Cipher FeedBack Mode
  - Se utilizado o modo CBC existiria duas opções:
    - Transmitir imediatamente, completando os restants dos bits com zero. (Sobrecarga de comunicação).
    - Transmitir somente quando fosse completado 64 bits de dados. (impossível de utilizar em algumas aplicações)
  - Problemas:
    - A criptografia de um bloco do plaintext Pi, é realziada em função das encriptações anteriores (misturados XOR).
    - Se o ciphertext transmitido corromper 1 bit, toda a mensagem a partir desse ponto é afetada.

19

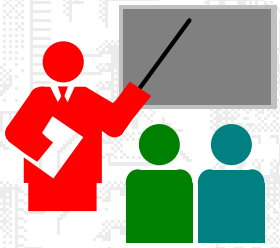
MODOS DE OPERAÇÃO DO DES

- OFB: Output FeedBack Mode
- Similar ao CFB
- Erros na transmissão não são propagados, não inviabilizando a decriptação do restante da mensagem.

20

ALGORITMOS MODERNOS

Triplo DES
AES



21

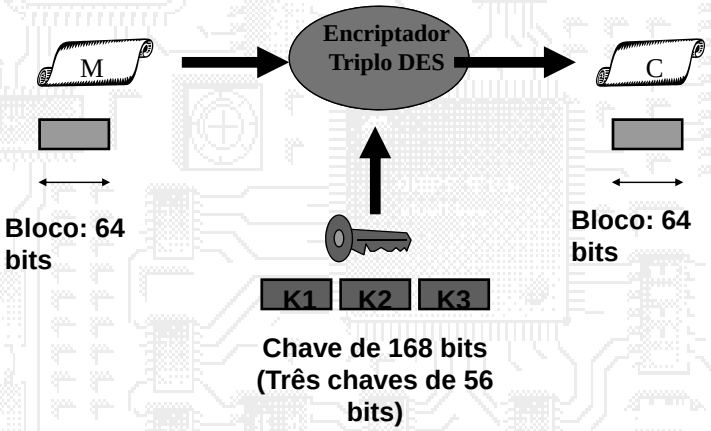
Triplo DES (3-DES)

- Dois tipos de implementação
  - Com chave de 168 bits (3 chaves de 56 bits)
  - Com chave de 112 bits (2 chaves de 56 bits)
    - Segundo estágio é uma decriptação
    - Permite manter compatibilidade com DES simples. Neste caso basta fazer $K_1 = K_2$.

22

Triplo DES de 168 bits

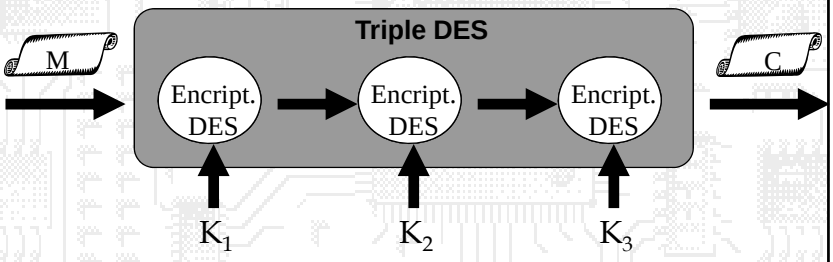
- Triplo DES de 3 chaves de 56 bits



23

Triplo DES de 168 bits (2)

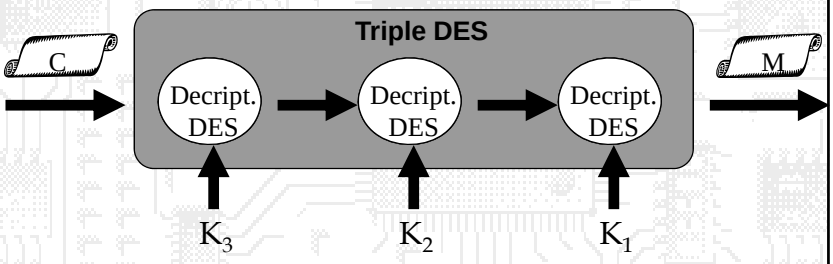
- Encriptação
  - $C = E_{k3} [E_{k2} [E_{k1} [M]]]$



24

Triplo DES de 168 bits (3)

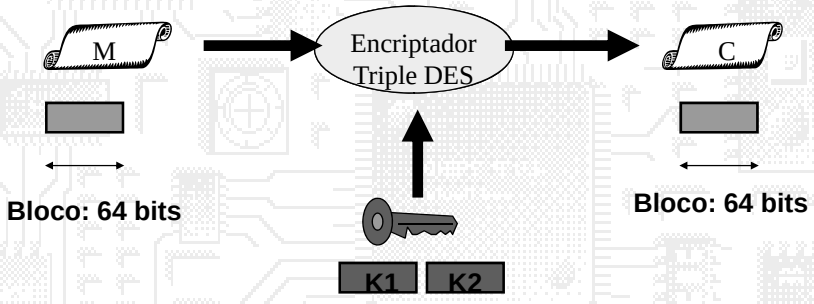
- Decriptação
  - $M = D_{k1} [D_{k2} [D_{k3} [C]]]$



25

Triplo DES de 112 bits (1)

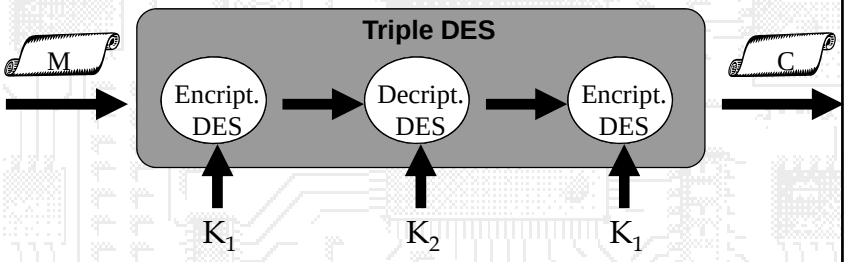
- Triple DES de 2 chaves de 56 bits



26

Triplo DES de 112 bits (2)

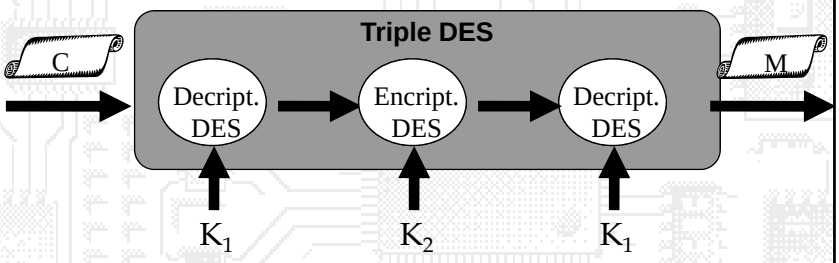
- Encriptação
  - $C = E_{k_1} [D_{k_2} [E_{k_1} [M]]]$



27

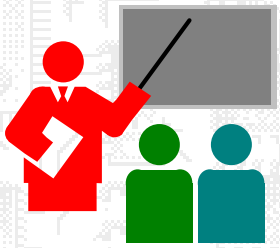
Triplo DES de 112 bits (3)

- Decriptação
  - $M = D_{k_1} [E_{k_2} [D_{k_1} [C]]]$



28

ALGORITMO IDEA



29

ALGORITMO IDEA

- International Data Encription Algorithm
- Desenvolvido por Xuejia Lai & James Massey
- “Swiss Federal Institute of Technology”, Zurich, 1991
- Patenteado mas com permissão para uso não comercial.
- Considerado “forte”.

30

IDEA - PRINCIPAIS CARACTERÍSTICAS

- Comprimento do bloco:
  - Deve ser longo o suficiente para deter análise estatística
  - Blocos de 64 bits.
- Comprimento da chave:
  - Deve ser longa o suficiente para prevenir força bruta
  - Chaves de 128 bits

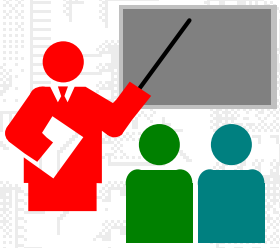
31

IDEA - PRINCIPAIS CARACTERÍSTICAS (2)

- "Confusão"
  - O relacionamento ciphertext-plaintext deve ser o mais complexo possível
  - Utiliza XOR, aritmética modular (+, *)
- "Difusão"
  - Cada bit do plaintext deve influenciar todos os bits do ciphertext
  - Cada bit da chave deve influenciar todos os bits do ciphertext

32

ALGORITMO AES



33

AES - O Mais Novo (2002)

- AES - *Advanced Encryption Standard*
  - Algoritmo selecionado**: RIJNDAEL**
- **Novo padrão** FIPS (*Federal Information Processing Standard*) escolhido pelo NIST (*National Institute of Standards and Technologies*) para ser utilizado pelas organizações governamentais dos EUA na proteção de informações sensíveis
- Marca um esforço de 4 anos de cooperação entre o governo dos EUA, empresas privadas e pesquisadores de diversos países

34

AES - Breve Histórico

- 1997: NIST requisita propostas
- 1998: Round 1: São selecionados inicialmente 15 algoritmos
- 1999: Round 2: Foram selecionados os algoritmos finalistas. Dos 15 pre-selecionados, foram 5 finais
- Out 2000: Anúncio do algortimo selecionado:
  - **RIJNDAEL**

35

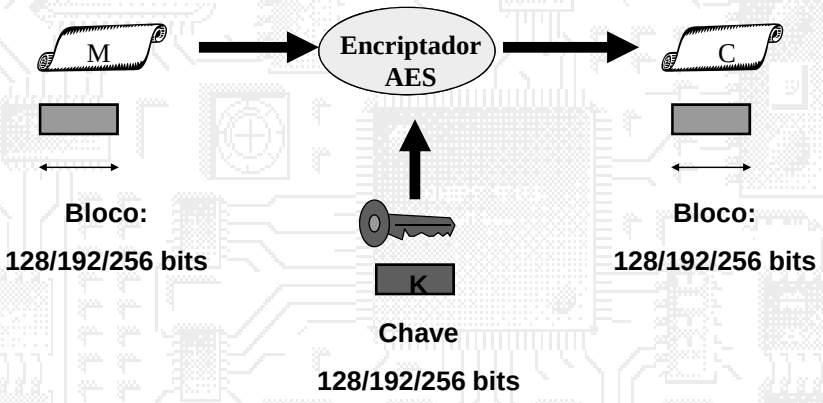
AES - Histórico - Ano 2000

- Nov 2000: Liberação do Draft do algoritmo AES
- Fev 2001: Término do período para comentários
- HOJE: ????
- Atualmente:
  - Anúncio do padrão FIPS
  - Mais informações: **www.nist.gov/aes**

36

AES - RIJNDAEL

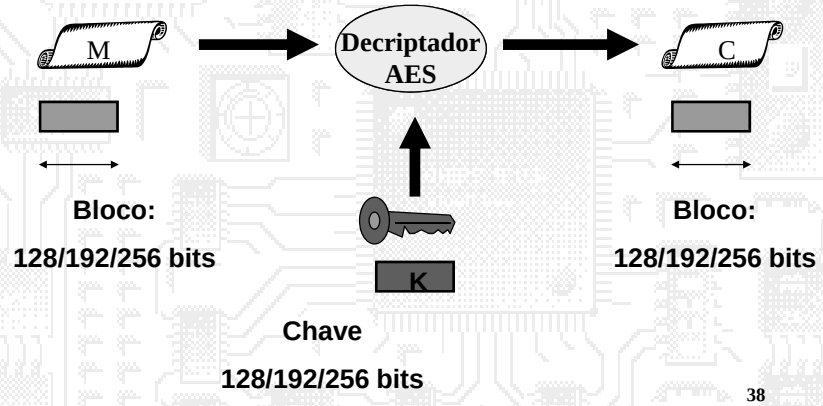
- Encriptação



37

AES - RIJNDAEL (2)

- Decriptação



38

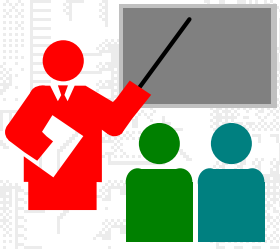
Principais Algoritmos Simétricos

Algoritmo	Projetista	Key (bits)	Bloco (bytes)	Aplicação
AES	J. Daemen, V. Rijmen	128, 192, 256	16	DMSEnvoy
Blowfish	Bruce Schneier	<= 448	8	Norton Utilities
3DES	D. Coppersmith	168	8	SSL, SSH
IDEA	X Lai, J. Massey	128	8	PGP, SSH, SSL
RC6	R. Rivest, M. Robshaw, et al.	128, 192, 256	16	AES candidato
STREAM		KEY		
RC4	R. Rivest	Mínimo 8, máximo 2048 em múltiplo de 8 bits Default: 128		SSL
SEAL	P. Rogaway	Variável, Default: 160		Disk Encryption

39

CONFIDENCIALIDADE

Usando Criptografia Convencional



40

CONFIDENCIALIDADE NO TRÁFEGO

- Identificação dos Parceiros
- Freqüência de Comunicação entre os parceiros
- Padrão, comprimento e quantidade de mensagens
- Eventos correlacionados

BIBLIOGRAFIA

- Stallings, William. **Cryptography and Network Security**: Principles and Practice. Prentice Hall, 1999. 569p.
- Tanenbaum, Andrew S. **Computers Networks**. 3rd Edition, New Jersey: Prentice Hall, 1996. 813p. Cap. 7: The Application Layer, p.577-766.
- RSA Data Security, Inc. "**Frequently Asked Questions about Today's Cryptography**". 1998. http://www.rsa.com.
- Soares, Luiz F. G.; Lemos, Guido; Colcher, Sérgio. **Redes de Computadores**: Das LANs, MANs e WANs às Redes ATM. 2ª Edição, Rio de Janeiro: Ed. Campus, 1995. 740p. Cap. 17: Segurança em Redes de Computadores, p.447-488.
- Schneier, Bruce. **Applied Cryptography**: Protocols, Algorithms, and Source Code in C. 2sd Edition, New York: John Wiley & Sons, 1996. 758p.

11/22/2010