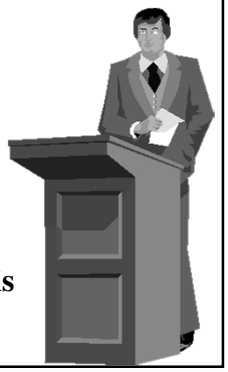
Criptografia Simétrica

Prof. Dr. Volnys Borges Bernal[2]
Prof. Dr. Adilson Eduardo Guelfi[1]

(1) Faculdade de Informática de PP
UNOESTE

(2) Laboratório de Sistemas Integráveis
Escola Politécnica da USP



Agenda

- Modelo de Criptografia Simétrica
- Principais Algoritmos de Criptografia Simétrica
- Criptografia Simétrica - DES
- Criptografia Simétrica - 3DES
- Criptografia Simétrica – AES
- Exercícios
- Referências Bibliográficas

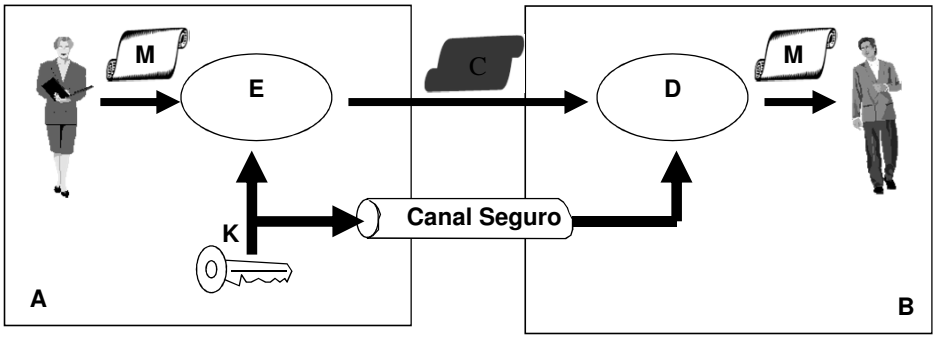
Modelo de Criptografia Simétrica

Modelo de Criptografia Simétrica

- **Um esquema de criptografia simétrica possui 5 elementos:**
  - Texto Legível: mensagem ou dados originais, inteligíveis e adotados como entrada no processo de cifração
  - Algoritmo de Cifração (Criptografia)
  - Chave Secreta: valor independente, aleatório, adotado como entrada no processo de cifração e participa das substituições e transformações realizadas pelo algoritmo
  - Texto Cifrado: mensagem embaralhada, ininteligível e produzido como saída do processo de cifração
  - Algoritmo de Decifração: toma como entradas a chave e o texto cifrado e produz como saída o texto legível original

Modelo de Criptografia Simétrica

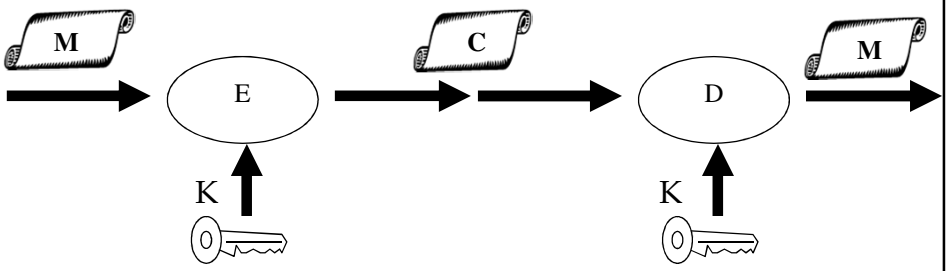
- **Modelo Completo de Criptografia Simétrica - Notação**
  - Texto legível ou Mensagem = M
  - Chave Criptográfica = K
  - Texto cifrado ou Criptograma = C



Modelo de Criptografia Simétrica

- **Requisitos para uso seguro da criptografia simétrica**
  - Algoritmo de criptografia forte
    - Quem conhece o algoritmo deve ser incapaz de decifrar o texto cifrado ou descobrir a chave secreta
    - Resistência a ataques (criptoanálise, por mensagens escolhidas, força bruta etc.)
  - Emissor e receptor compartilham chave secreta de forma segura e precisam manter a chave protegida
  - Deve ser impraticável decifrar uma mensagem com base no texto cifrado mais o conhecimento do algoritmo
  - Apenas a chave deve ser secreta (independentemente do algoritmo)
    - **Principal problema de segurança = manter o sigilo da chave**

Modelo de Criptografia Simétrica



- **Criptografia ou cifração C = E (K, M)**
  - Texto cifrado **C** é produzido pelo algoritmo de cifração **E** como função da chave **K** e do texto legível **M**
- **Decifração M = D (K, C)**
  - Texto legível **M** é produzido pelo algoritmo decifração **D** como função da chave **K** e do texto cifrado **C**.

Modelo de Criptografia Simétrica

- **Exemplo**
  - Criptografia simétrica com a função XOR desempenhando o papel de algoritmo de criptografia

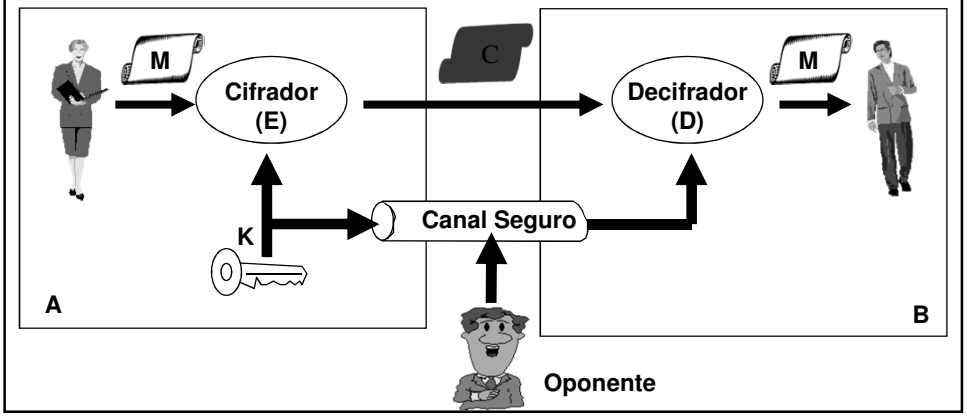
Texto Legível:	**10100011**	**Ciphertext:**	**00001000**
Chave:	**10101011**	**Chave:**	**10101011**
Ciphertext:	**00001000**	**Texto Legível:**	**10100011**

Tabela de XOR

⊕	0	1
0	0	1
1	1	0

Modelo de Criptografia Simétrica

- **Principal problema da criptografia simétrica:**
  - Distribuição da chave: chave secreta K deve ser passada por um canal seguro até o parceiro



Modelo de Criptografia Simétrica

- **Utilização da criptografia simétrica**
  - Confidencialidade
    - Esquema apropriado quando o algoritmo, tamanho da chave criptográfica e sua distribuição são considerados seguros
  - Autenticação
    - Esquema não muito apropriado pois a chave criptográfica simétrica (segredo) é compartilhada
  - Integridade – não aplicável
  - Irretratabilidade – idem item autenticação.

Principais Algoritmos de Criptografia Simétrica

Principais Algoritmos

Nome	Tipo	Tam. chave	Tam. bloco
DES	bloco	56	64
Triple DES (2 ch.)	bloco	112	64
Triple DES (3 ch.)	bloco	168	64
IDEA	bloco	128	64
BLOWFISH	bloco	32 a 448	64
RC5	bloco	0 a 2040	32,64,128
CAST-128	bloco	40 a 128	64
RC2	bloco	0 a 1024	64
RC4	stream	0 a 256	--
Rijndael (AES)	bloco	128,192,256	128, 192, 256
Twofish	bloco	128,192,256	128

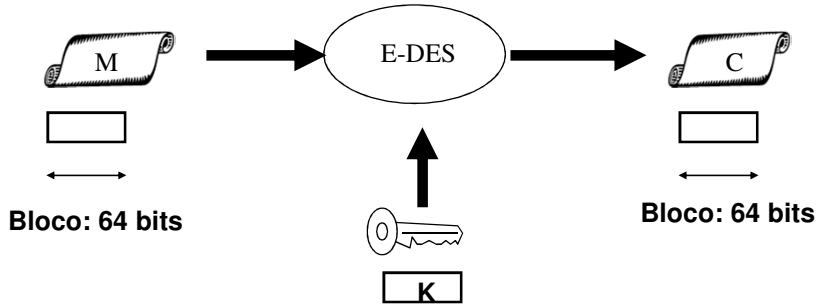
Criptografia Simétrica - DES

DES

- **DES - "*Data Encryption Standard*"**
- **Padrão de criptografia adotado em 1977 pelo NIST**
  - Primeiro padrão de criptografia para entidades do governo federal dos EUA
  - Documentos FIPS
    - FIPS PUB 46-3 – DES
    - FIPS 74 – Guia de implementação e uso do DES
    - FIPS 81 – *DES modes of operation*
  - FIPS (*Federal Information Processing Standard*)
- **Para o DES, dados são codificados em blocos de 64 bits usando uma chave de 56 bits**

DES

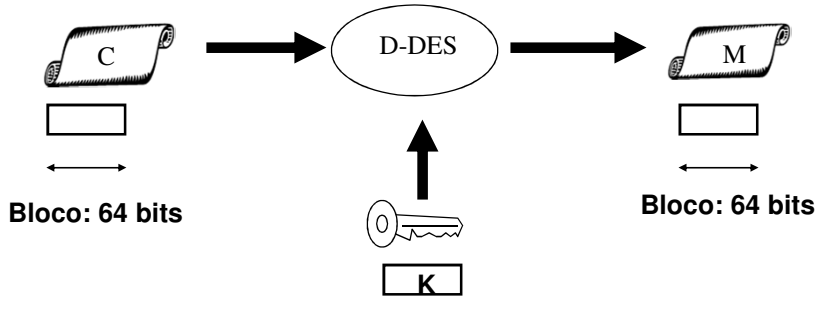
- **Cifração**



Chave de tamanho igual à 56 bits

DES

- **Decifração**



Chave de tamanho igual à 56 bits

DES

- **Problemas**
  - Atualmente o DES é considerado um algoritmo **extremamente inseguro**, principalmente para transações financeiras

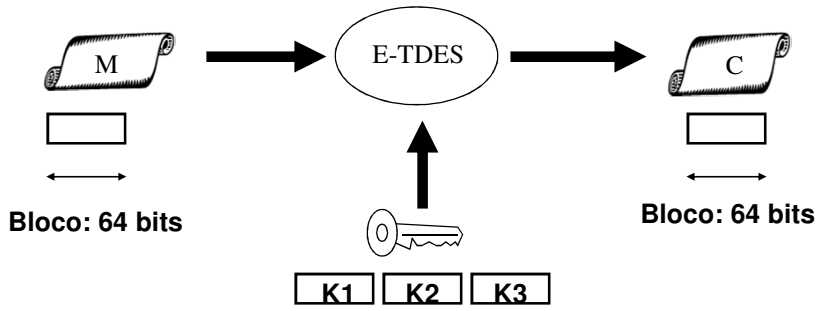
Criptografia Simétrica – 3DES

Triple DES

- **Caso particular de criptografia múltipla com 3 estágios DES utilizando chaves diferentes**
- **Duas configurações diferentes para o Triple DES**
  - Chave de 168 bits (3 chaves DES de 56 bits)
  - Chave de 112 bits (2 chaves DES de 56 bits)

Triple DES

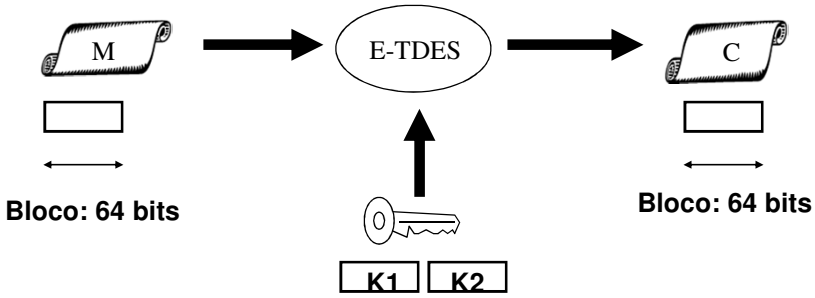
- **Triple DES de 3 chaves de 56 bits**



Chave de tamanho igual à 168 bits
(Três chaves de 56 bits)

Triple DES

- **Triple DES com 2 chaves de 56 bits**



Chave de tamanho igual à 112 bits
(Duas chaves de 56 bits)

Criptografia Simétrica - AES

AES

- **AES - *Advanced Encrypton Standard***
  - Cifra em bloco simétrica
  - Novo (segundo) padrão de criptografia para entidades do governo federal dos EUA
  - Publicado pelo NIST (FIPS - EUA) em 2001
  - Documento FIPS PUB 197
- **Marca um esforço de 4 anos de cooperação entre governo dos EUA, empresas e pesquisadores de diversos países**

AES

- **Breve Histórico**
  - 1997 - NIST requisita propostas de algoritmos com grau de segurança igual ou superior ao 3DES e uma eficiência bem melhorada
  - Round 1: 15 algoritmos propostos
  - NIST selecionou o RIJNDAEL como AES proposto
  - 2001 - Anúncio do padrão oficial FIPS PUB 197

AES

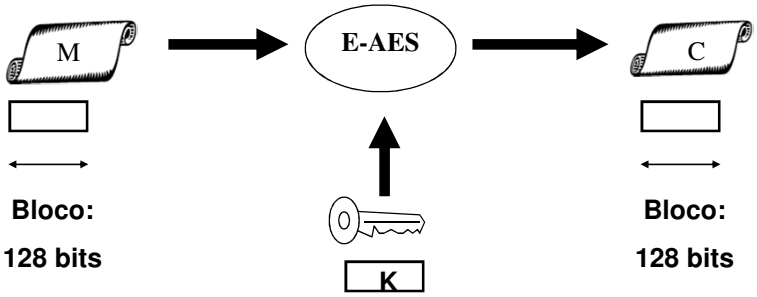
- **Critérios NIST para avaliar e escolher o AES**
  - Segurança
    - Segurança Real (resistência à ataques conhecidos de criptoanálise diferencial e linear), Aleatoriedade, Solidez (da base matemática para a segurança) e Outros Fatores de Segurança
  - Custo
    - Condições de Licenciamento (sem royalties) Alta Eficiência Computacional, Requisitos de Memória
  - Algoritmo e Características de Implementação
    - Flexibilidade (tamanhos adicionais de chave e bloco, uso em diversas plataformas etc), Adequação de Hardware e Software, Simplicidade (do projeto)

AES

- **Funcionamento do algoritmo**
  - AES pode ser operado de forma que o tamanho do bloco e o tamanho da chave podem ser especificados independentemente com valores de 128, 192 ou 256 bits
  - A especificação do AES limitou o tamanho de bloco em 128 bits mas preservou o tamanho de chave nas três alternativas possíveis, ou seja, 128, 192 ou 256 bits

AES

- **Cifração**

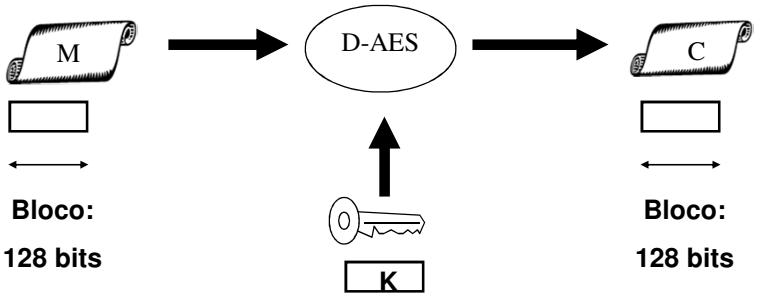


Chave Criptográfica

128/192/256 bits

AES

- **Decifração**



Chave Criptográfica

128/192/256 bits

Exercícios

Exercício

(1) OpenSSL é uma biblioteca criptográfica aberta e extremamente versátil. É utilizada atualmente em diversos sistemas comerciais. Além do conjunto de funções, a biblioteca também disponibiliza alguns utilitários.

Utilize o utilitário openssl para cifrar um arquivo utilizando o algoritmo DES no modo ECB. Para isto, abra uma janela de comandos e execute o seguinte comando:

```
openssl enc -des-ecb -in <arq> -out <criptograma>
```

Exercício

(2) Utilize o utilitário openssl para decifrar o criptograma gerado no exercício anterior.

(3) Com o utilitário openssl, repita os exercícios (1) e (2) de cifrar e decifrar escolhendo outros algoritmos de criptografia simétrica como o 3DES, AES, RC4 etc.

Referências Bibliográficas

Referências Bibliográficas

- **Criptografia e Segurança de Redes - Princípios e Práticas (4a. Edição)**
  - Willian Stallings, Pearson. 2008
- **APPLIED CRYPTOGRAPHY - PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C**
  - SCHNEIER, BRUCE, Editora: JOHN WILEY CONSUMER, Edição: 2ª, 1996

Referências Bibliográficas

- **Sites Recomendados – Procurar por:**
  - Crypto Corner
  - Computer Security Resource Center (NIST – procurar pelos FIPS Special Publications)
  - SANS Institute
  - The AES Lounge
  - Vídeos YouTube – AES, DES e Enigma Machine