

Criptografia e Segurança de Dados

Prof. Dr. Daniel Vecchiato

Objetivo da disciplina

A disciplina se propõe a trabalhar métodos para comunicações secretas fundamentados na aplicação da matemática discreta e algoritmos de chave pública e privada

Ementa

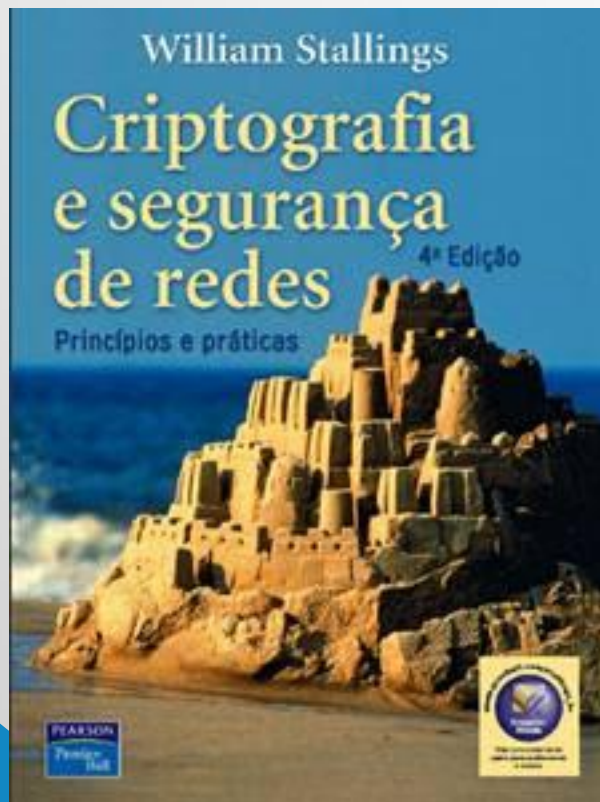
- Segurança de Dados, Sistemas de Criptografia, Aritmética Modular, Teoria dos Números, Tipos Cifras, Algoritmos Fundamentais, Criptografia de Chave Pública e Privada, Assinatura Digital

Pré-requisito

- Algoritmos II
- Laboratório de Programação

Bibliografia básica

- Criptografia e Segurança de Redes – William Stallings – 6ª edição



Conteúdo programático

- Aula 01 – Segurança de Dados e Sistemas de Criptografia
- Aula 02 – DES, AES, RC₄, Modos de operação de Cifra
- Aula 03 – RSA, Chave Pública, Certificados Digitais
- Aula 04 – Avaliação

Método de avaliação

Média = $(1^{\text{a}} \text{ Avaliação} + \text{Trabalho 1} + \text{Trabalho 2} + \text{Trabalho 3})/4$

Se (média ≥ 5) então

Aprovado

Senão

Reprovado

Segurança de dados

A decorative graphic in the bottom right corner consisting of several parallel lines in blue and grey, creating a sense of depth and movement.

Por que se preocupar com segurança?

Problemas mais comuns:

Destruição de informações e outros recursos.

Modificação ou deturpação de informações.

Roubo, remoção ou perda da informação ou de outros recursos.

Revelação de informações.

Interrupção de serviços.

Segurança da Informação

- Segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança

Informação

- Essencial para o sucesso do negócio
- Existente em muitas formas
 - Impressa
 - Escrita
 - Armazenada em um computador
 - Na “cabeça” de alguém
 - Etc...
- A informação sempre deve ser protegida adequadamente

Criptografia

- Algoritmos de criptografia podem ser agrupados em quatro principais áreas:
 - Encriptação simétrica
 - Encriptação assimétrica
 - Algoritmos de integridade de dados
 - Protocolos de autenticação

Segurança da Informação

- Geralmente é referenciada sob 3 pilares (CID)
 - Confidencialidade
 - Integridade
 - Disponibilidade



Confidencialidade

- Compreende a proteção de dados transmitidos contra ataques passivos, isto é, contra acessos não autorizados, envolvendo medidas como controle de acesso e criptografia.
- A perda da **confidencialidade** ocorre quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.

Integridade

- Trata da garantia contra ataques ativos por meio de alterações ou remoções não autorizadas. É relevante o uso de um esquema que permita a verificação da integridade dos dados armazenados e em transmissão.
- Uma vez que os ataques ativos são considerados no contexto, a detecção, ao invés da prevenção, é o que importa; então, se o comprometimento da integridade é detectado, pode-se reportá-lo e o mecanismo de recuperação é imediatamente acionado.

Disponibilidade

- Determina que recursos estejam disponíveis para acesso por entidades autorizadas, sempre que solicitados, representando a proteção contra perdas ou degradações.
- A perda de **disponibilidade** acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

Complementando a segurança

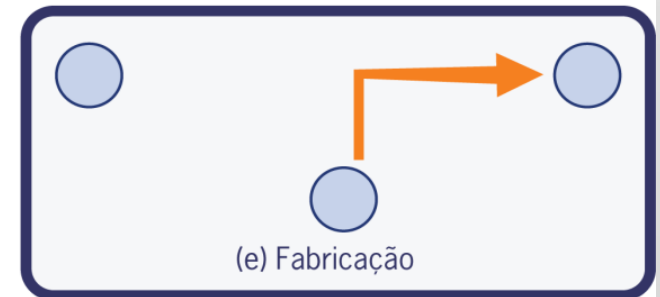
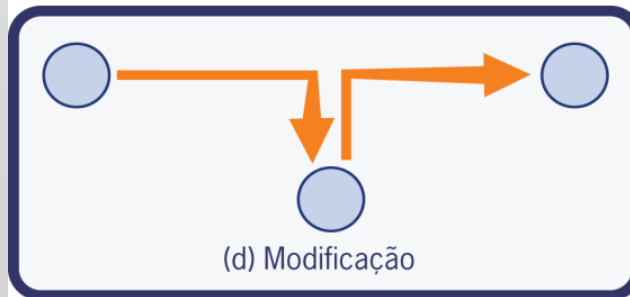
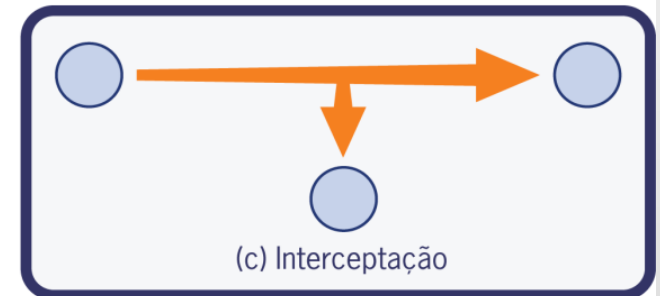
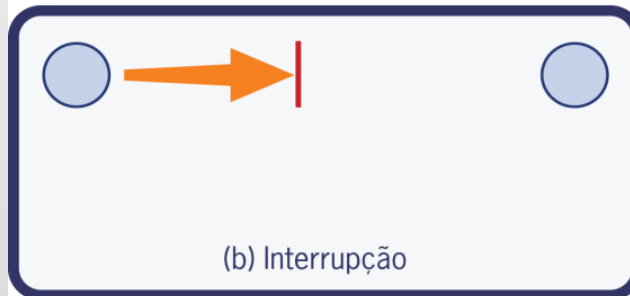
- Não repúdio
 - Compreende o serviço que previne uma origem ou destino de negar a transmissão de mensagens, isto é, quando dada mensagem é enviada, o destino pode provar que esta foi realmente enviada por determinada origem, e vice-versa.
- Autenticidade
 - Esta preocupada em garantir que uma comunicação é autêntica, ou seja, origem e destino podem verificar a identidade da outra parte envolvida na comunicação, com o objetivo de confirmar que a outra parte é realmente quem alega ser.
 - A origem e o destino tipicamente são usuários, dispositivos ou processos.

Aspectos da Segurança

- As portas dos fundos são tão boas quanto as portas da frente
- Uma corrente é tão forte quanto ao seu elo mais fraco
- Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável



Modelos de ataques



Tipos de Ataques

- DoS – Denial of Service
- DDoS – Distributed Denial of Service
- Força Bruta
- Sniffing
- Engenharia Social

Desafios para a segurança

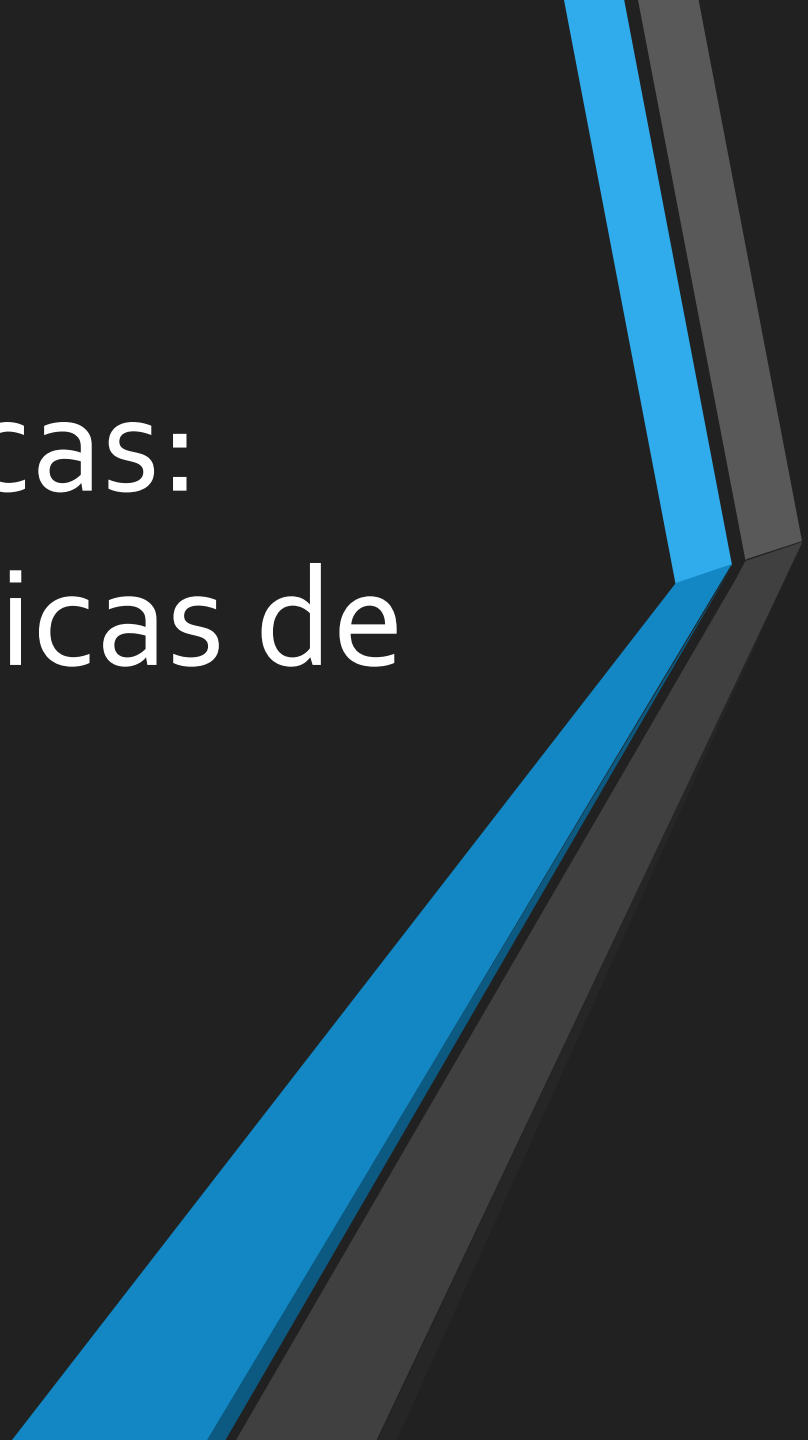
- Dispositivos móveis
- Redes sem fio
- Computação em nuvem
- Identificar e fortalecer o elo mais fraco

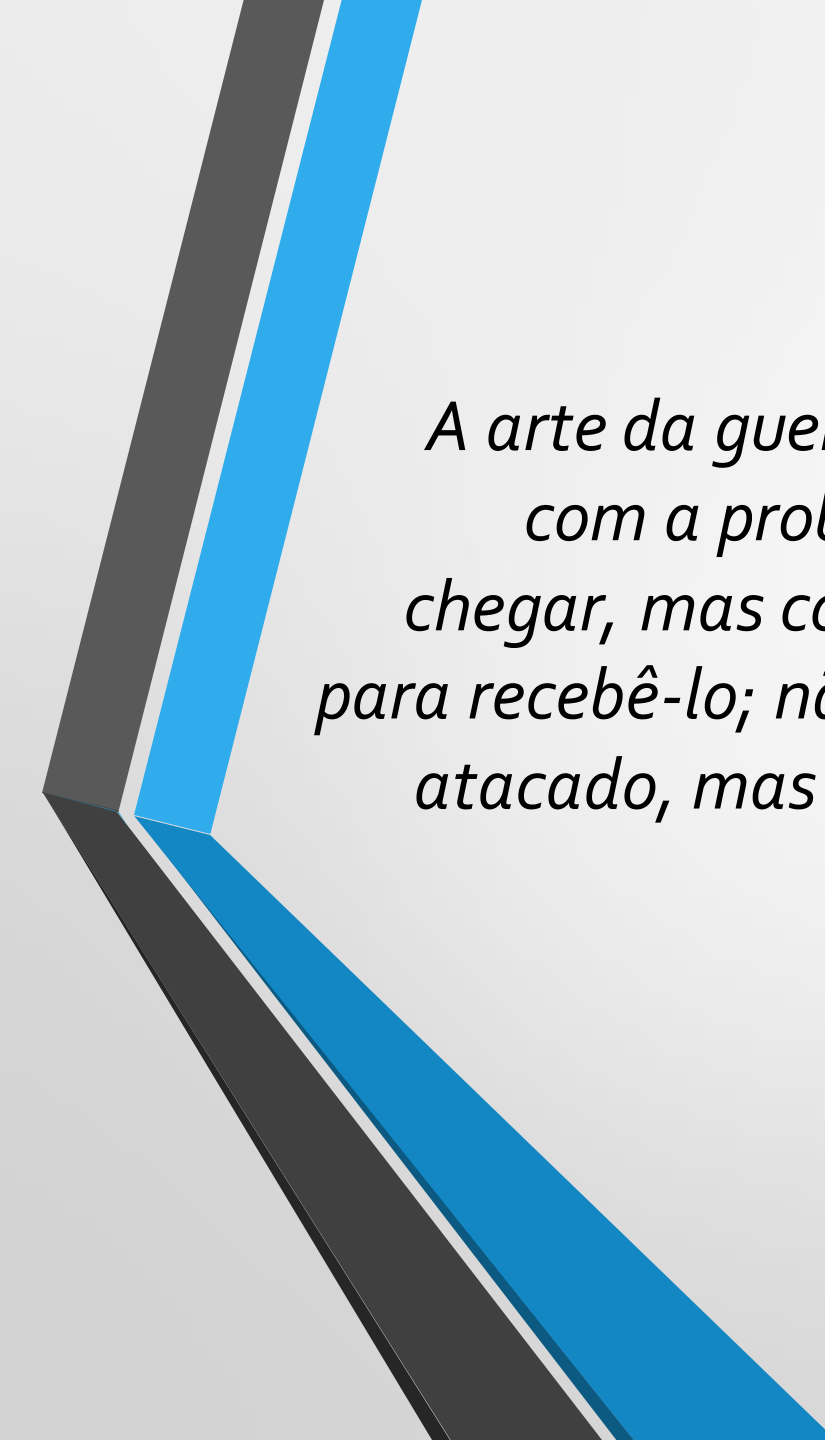


Relembrando!

- O que é ataque de força bruta?
- O que é integridade?
- O que é disponibilidade?
- O que é confidencialidade?
- Qual é a diferença entre ataque de modificação e fabricação?

Cifras Simétricas: Técnicas Clássicas de Encriptação





A arte da guerra nos ensina a contar não com a probabilidade de o inimigo não chegar, mas com nossa própria prontidão para recebê-lo; não com a chance de não ser atacado, mas com o fato de tornar nossa posição inatacável.

A arte da guerra, Sun Tzu

Conceitos

- Texto claro = mensagem original
- Texto cifrado = mensagem codificada
- Cifragem ou Criptografia = processo de converter o **texto claro** em **texto cifrado**
- Decifragem ou Decriptografia = restaurar o texto claro a partir do texto cifrado
- Criptoanálise = técnicas empregadas para decifrar uma mensagem sem qualquer conhecimento dos detalhes de criptografia

Criptologia = criptografia + criptoanálise

Criptografia Simétrica

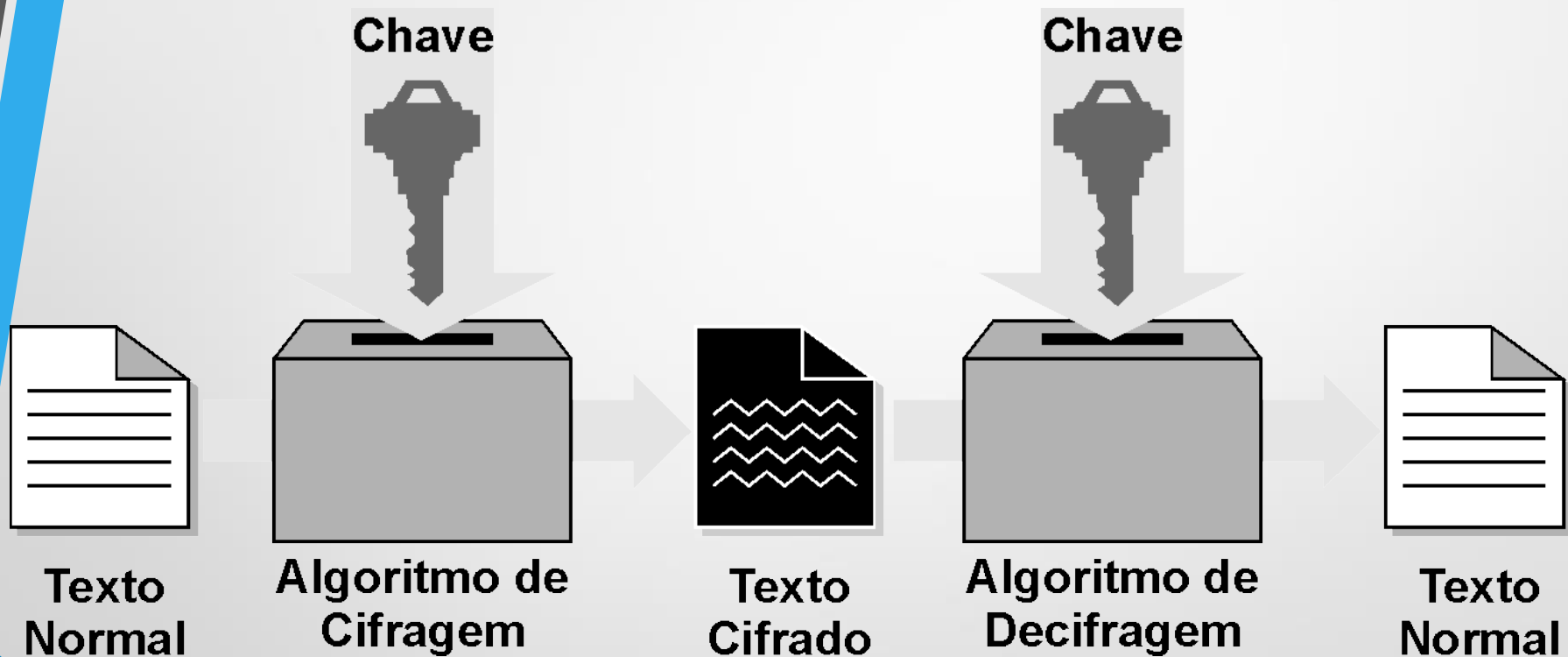
- Também chamada de:
 - Convencional
 - De Chave Única
 - De Chave secreta
- O mais usado dos dois tipos de encriptação

Modelo de cifra simétrica

- Possui cinco “ingredientes”:
 - Texto claro
 - Algoritmo de criptografia
 - Chave secreta
 - Texto cifrado
 - Algoritmo de decriptografia



Modelo de cifra simétrica



Modelo de cifra simétrica

- O algoritmo pode ser de conhecimento público
- Apenas o texto cifrado e o algoritmo de (de)cifragem não são suficientes para obter o texto claro
- A segurança reside no sigilo da chave
- Notação:
 - Texto cifrado = criptografia (Chave, Texto claro)
 - Texto claro = decriptografia (Chave, Texto cifrado)

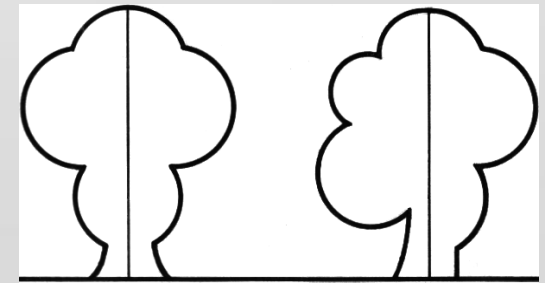
Modelo de cifra simétrica

- Os sistemas criptográficos são caracterizados em três dimensões independentes:
 1. Tipo das operações usadas para a criptografia
 - *Substituição*: cada elemento no texto claro é mapeado em outro elemento
 - *Transposição*: os elementos no texto claro são reorganizados.



Modelo de cifra simétrica

- Os sistemas criptográficos são caracterizados em três dimensões independentes:
 2. Número de chaves usadas:
 - **Chave simétrica** (única, secreta ou convencional): tanto o emissor quanto o receptor utilizam a mesma chave
 - **Chave assimétrica** (duas chaves, chave pública): o emissor e receptor usam chaves diferentes.



Modelo de cifra simétrica

- Os sistemas criptográficos são caracterizados em três dimensões independentes:
 3. Modo como o texto claro é processado
 - **Cifra de bloco**: processa a entrada de um bloco de elementos de cada vez, produzindo um bloco de saída para cada bloco de entrada.
 - **Cifra em fluxo**: processa os elementos da entrada continuamente, produzindo a saída de um elemento de cada vez, enquanto prossegue.

Criptanálise

- Normalmente o objetivo é recuperar a chave em uso
- Existem duas estratégias gerais para o ataque:
 - *Criptanálise*: utilização de conhecimentos como a natureza do algoritmo, trechos do texto claro, texto criptografado.
 - *Ataque por força bruta*: tentativa e erro até descobrir a chave.

Criptanálise

- Pode-se utilizar conhecimento:
 - da língua que o texto está escrito
 - de trechos do texto claro
 - linguagem de programação, em caso de código fonte
 - Entre outras...
- Somente algoritmos relativamente fracos não conseguem resistir a um ataque apenas de texto cifrado. Em geral, são projetados para resistir um ataque de texto claro conhecido

Criptanálise

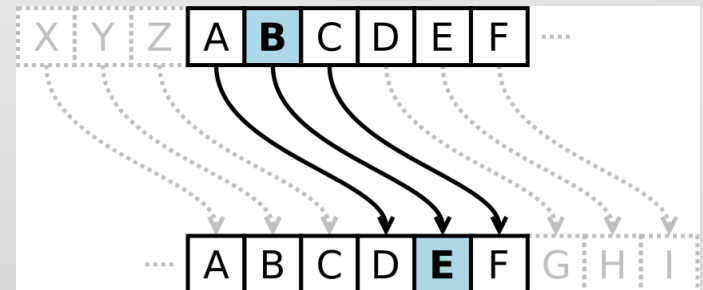
- Um esquema de criptografia é **incondicionalmente seguro** se o texto cifrado gerado pelo esquema não tiver informações suficientes para determinar exclusivamente o texto claro correspondente.
 - One-Time Pad
 - Na prática é impossível
- Um esquema é considerado computacionalmente seguro se um desses dois critérios for atendido:
 - Custo para quebrar a cifra for superior ao valor da informação codificada
 - Tempo exigido para quebrar a cifra for superior ao tempo de vida útil da informação

Relembrando!

- O que é substituição?
- O que é transposição?
- O que é criptografia convencional?
- O que é criptografia de chave pública?
- Quais são os ingredientes essenciais de uma cifra simétrica?

Técnicas de substituição

- Cifra de César
 - Uso mais antigo que conhecemos de uma cifra de substituição. Feita por Júlio César.
 - Consiste na substituição das letras da mensagem pelas letras que se encontram um número fixo de vezes a frente no alfabeto
 - A cifra de César utiliza $K = 3$



Cifra de César

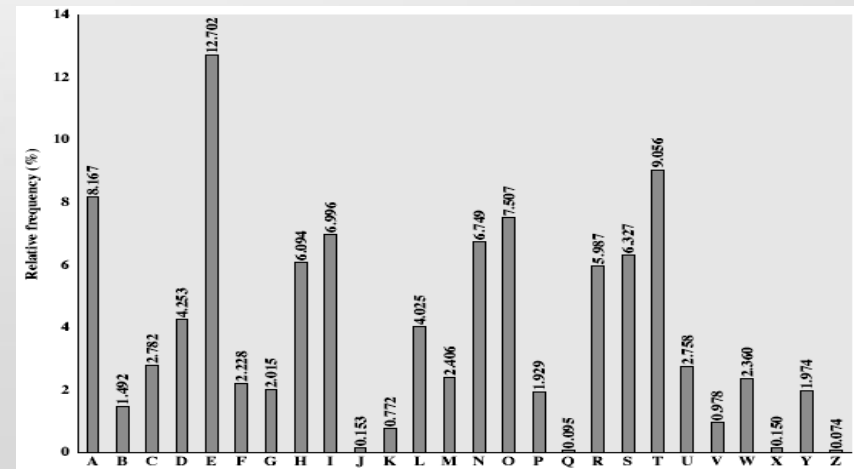
- Decodifique a seguinte cifra usando $k=3$
 - DYH FDHVDU
 - AVE CAESAR
- O desafio proposto consistia na cifra de César

Cifra de César

- Problemas:
 - Algoritmos de criptografia e descriptografia são conhecidos
 - Existem apenas 25 chaves a serem experimentadas
 - A linguagem do texto claro é conhecida e facilmente reconhecível

Cifras monoalfabéticas

- Melhoramento da cifra de César, que continha 25 chaves possíveis
- Na **cifra por substituição monoalfabética** a substituição é arbitrária.
- 4×10^{26} chaves possíveis
- Porém...



Cifra Playfair

- Trata digramas como unidades isoladas
- Oculta completamente as frequências de única letra
- Baseado no uso de uma matriz (5x5) + palavra chave

Cifra Playfair

- Se um par repetir letra, a letra x é inserida
 - Ex. SUCESSO = SU CE SX SO
- Se ambas letras caírem na mesma linha, troque-as pela letra imediatamente a direita
 - De forma circular
- Se ambas letras caírem na mesma coluna, troque-as pela letra imediatamente abaixo
 - De forma circular
- Senão a letra é trocada pela letra que esta em sua linha e que está na mesma coluna de seu par

Cifra Playfair

M	O	V	E	L
A	B	C	D	F
G	H	I	J	K
N	P	Q	R	S
T	U	W	X	Y/Z

COMPUTACAO
=
BVONWUBDBM

Cifra Playfair

- Mais segura que a monoalfabética (26x26 digramas)
- Análise de frequência é mais difícil
 - Alguns pares são comuns, ex: TR, LH, etc.

Cifras polialfabéticas

- Cifra de Vigenère
 - Consiste em um conjunto de regras de substituição monoalfabéticas nas 26 cifras de César, com deslocamento de 0 a 25
 - Para criptografar a mensagem, é necessário que haja uma chave tão longa quanto a mensagem
 - Normalmente, a palavra chave é repetida

Chave: COMPUTACAOCOMPU

Texto claro: CIFRADEVIGENERE

Texto cifrado: EWRGUWEXIUGBQGY

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

One-Time Pad

- Chave de uso único
- Uso de uma chave aleatória do tamanho da mensagem
- Chave deve ser usada para criptografar e decriptografar uma única mensagem
- Sistema inquebrável
- A saída não possui nenhum relacionamento estatístico com o texto claro.

One-Time Pad

- A cifra de chave de uso único oferece segurança completa, mas, na prática, tem duas dificuldades fundamentais:
 - Criar grandes quantidade de chaves aleatórias
 - Distribuição e proteção de chaves
- Por causa dessas dificuldades, a cifra de chave de uso único tem utilidade limitada, e é útil principalmente para canais de pouca largura de banda, exigindo segurança muito alta.

Técnicas de transposição

- Permutação nas letras do texto claro
- Técnica de *rail fence*
 - $E\ T\ E\ M\ X\ M\ L$
 $S\ E\ U\ E\ E\ P\ O$
 - Saída: *ETEMXMLSEUEEPO*
- Técnica do retângulo
 - Chave: 3 4 2 1
 - Texto Claro: $E\ S\ T\ E$
 $E\ U\ M\ E$
 $X\ E\ M\ P$
 $L\ O$
 - Saída: *EEPTMMEEEXLSUEO*

Técnicas de transposição

- Podem ser aplicadas diversas vezes para aumentar a criptografia.
- Escondem formações de dígrafos
- O algoritmo DES trabalha com 16 estágios de transposição.

Esteganografia

- Escondem a existência da mensagem
 - Marcação de caractere: Letras selecionadas do texto impresso ou datilografado são sobrescritas por lápis
 - Tinta invisível: somente pode ser lida após utilização de química ou luz específica
 - Perfurações: Pequenos furos em letras selecionadas normalmente não são visíveis, a menos que o papel tenha uma fonte de luz no fundo
 - Fita corretiva de máquina de escrever
 - Uso de bits menos significativos de uma imagem

Relembrando!

- Qual é a diferença entre criptografia e esteganografia?
- Qual é a diferença entre uma cifra monoalfabética e uma polialfabética?
- Quais são os dois problemas da chave de uso único?
- Qual é a diferença entre uma cifra incondicionalmente segura e uma cifra computacionalmente segura?

Trabalho

- Individual
- Submeter no AVA
- Prazo: 09/12/2019 (Sem exceção)

Cifra de Bloco e o Data Encryption Standard



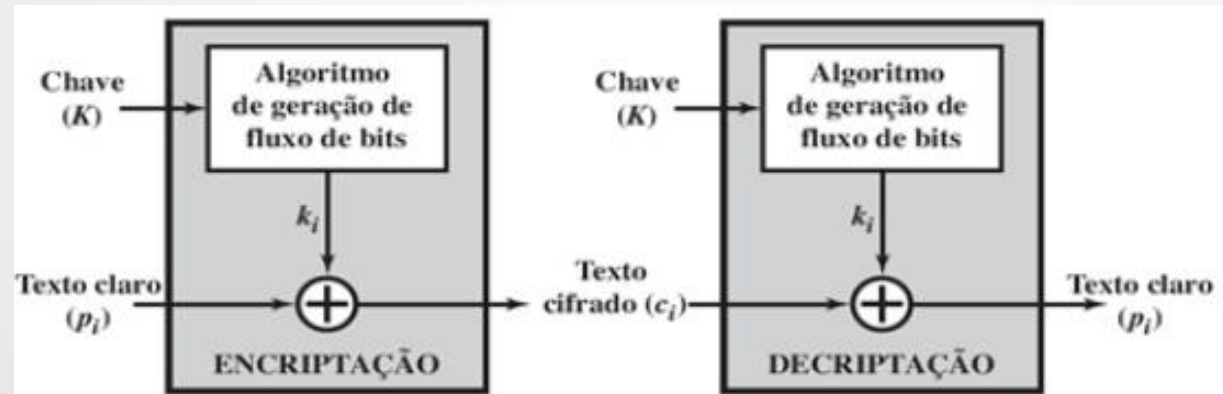
Cifras de Fluxo

- É aquela que encripta um fluxo de dados digital um bit ou um byte por vez
- Gerador de fluxo de bits precisa ser implementado como um procedimento algorítmico
- Usuários compartilham a chave de geração
 - Cada um produz o fluxo de chaves
- Ex: Vigenère, RC₄

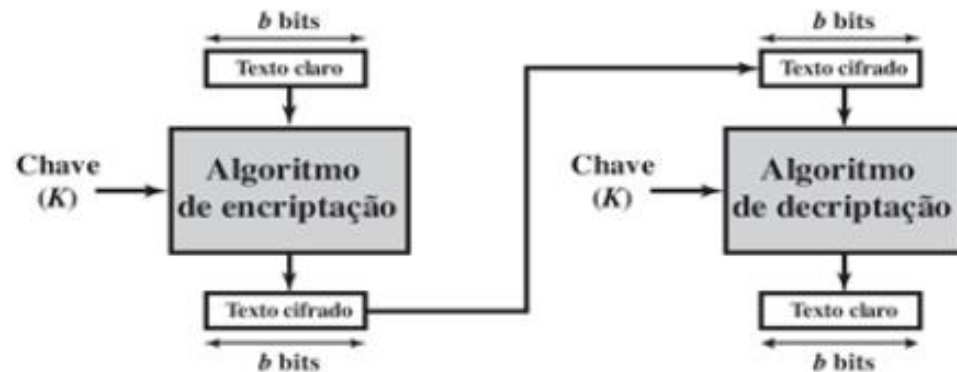
Cifras de Bloco

- Bloco de dados é tratado como um todo e usado para produzir um texto cifrado de mesmo tamanho
- Normalmente usa-se bloco de 64 ou 128 bits
 - Se bloco pequeno: Então é equivalente a uma cifra de substituição
 - Se bloco grande: então a implementação e desempenho são prejudicados
- Uma cifra de bloco pode ser utilizada para conseguir o mesmo efeito de uma cifra de fluxo.
- Maioria das aplicações de criptografia simétrica baseadas em rede utiliza cifras de bloco.

Cifra de Bloco vs Cifra de Fluxo



(a) Cifra de fluxo usando gerador algorítmico de fluxo de bits



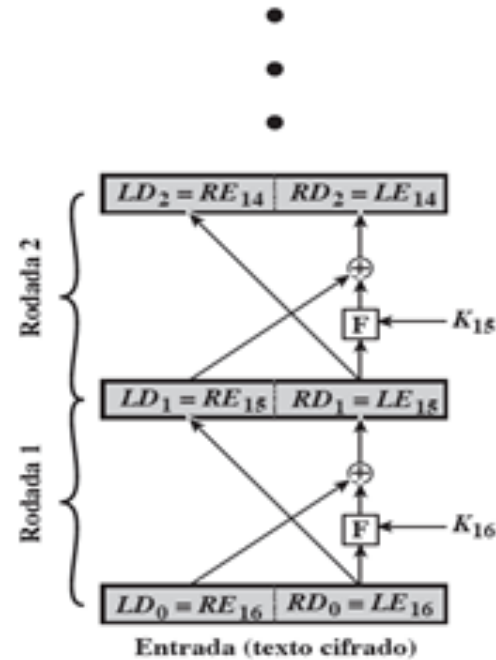
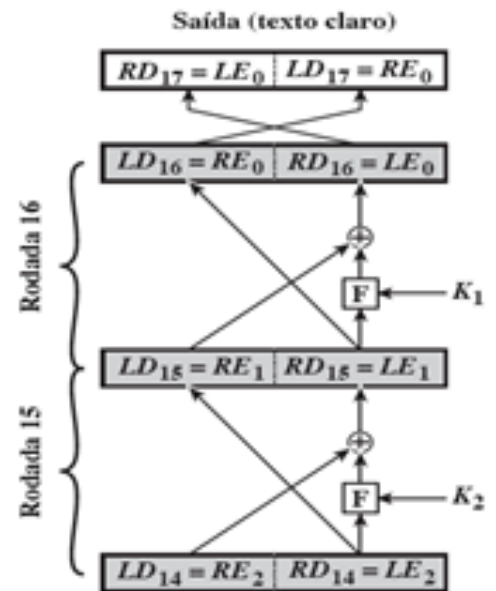
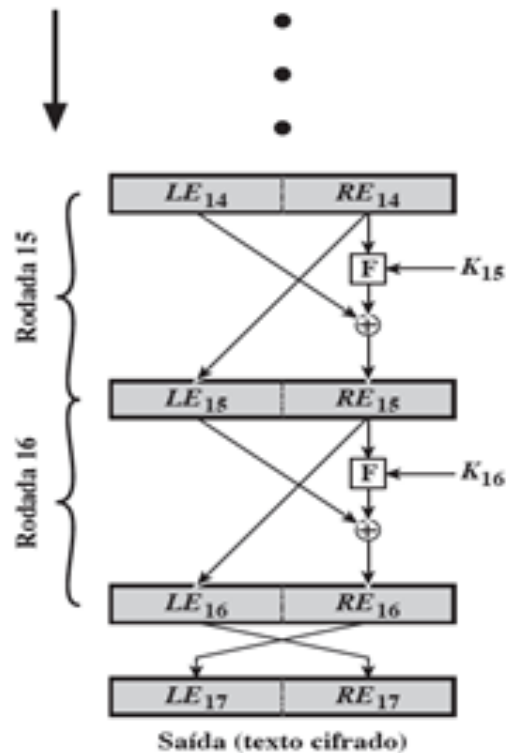
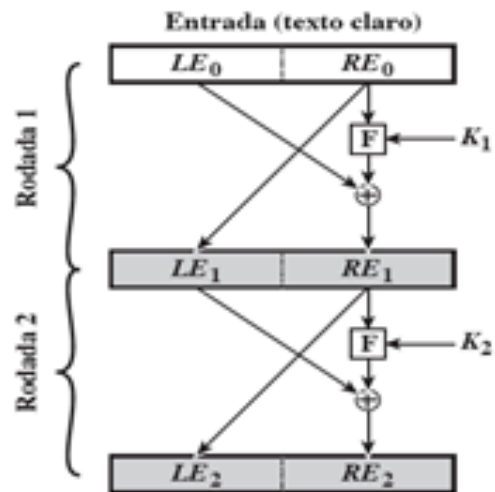
(b) Cifra de bloco

Cifra de Feistel

- Alterna substituições e permutações
 - Substituição: Cada elemento do texto claro é substituído exclusivamente por um elemento de texto cifrado
 - Permutação: Sequência de elementos em texto claro é substituída por uma permutação dessa sequência

Cifra de Feistel

- Parâmetros
 - Tamanho do bloco (64 a 128 bits)
 - Maior o bloco, maior a segurança e menor a velocidade
 - Tamanho de chave
 - Maior a chave, maior a segurança e menor a velocidade
 - Número de rodadas
 - Deve fazer com que a criptoanálise seja mais complexa que a força bruta
 - Algoritmo de geração de subchave
 - Maior complexidade = maior dificuldade de criptoanálise
 - Função F
 - Maior complexidade = maior dificuldade de criptoanálise
 - Oferece propriedade de confusão em uma cifra de feistel



Cifra de Feistel



OBS: Encriptação e Decriptação utilizam o mesmo algoritmo



DES

Data Encryption Standard

DES



Usa cifra de Feistel



bloco de 64 bits



chave de 56 bits

64 bits de entrada
56 bits usados (8 bits de paridade)
Chave de cada rodada tem 48 bits



Efeito avalanche

Pequena alteração no texto claro ou chave produz uma grande alteração no texto cifrado

Força do DES

Tamanho de chave (bits)	Cifra	Número de chaves alternativas	Tempo exigido a 10^9 decriptações/s	Tempo exigido a 10^{13} decriptações/s
56	DES	$2^{56} \approx 7,2 \times 10^{16}$	2^{55} ns = 1,125 ano	1 hora
128	AES	$2^{128} \approx 3,4 \times 10^{38}$	2^{127} ns = $5,3 \times 10^{21}$ anos	$5,3 \times 10^{17}$ anos
168	Triple DES	$2^{168} \approx 3,7 \times 10^{50}$	2^{167} ns = $5,8 \times 10^{33}$ anos	$5,8 \times 10^{29}$ anos
192	AES	$2^{192} \approx 6,3 \times 10^{57}$	2^{191} ns = $9,8 \times 10^{40}$ anos	$9,8 \times 10^{36}$ anos
256	AES	$2^{256} \approx 1,2 \times 10^{77}$	2^{255} ns = $1,8 \times 10^{60}$ anos	$1,8 \times 10^{56}$ ano
26 caracteres (permutação)	Monoalfabético	$2! = 4 \times 10^{26}$	2×10^{26} ns = $6,3 \times 10^9$ anos	$6,3 \times 10^6$ anos