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. Márcio H. C. d' Ávila, Tannenbaum, Kurose, Adriano Cansian entre outros)

TÓPICOS

- **Criptografia - Fundamentos**
  - Terminologia
  - Histórico
  - Conceitos Básicos

O que é Criptografia?

Criptografia

(*kriptos* = oculto + *graphos* = grafia)

"Arte ou a ciência de escrever em cifras (código)."

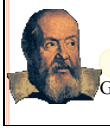
VISÃO GERAL

O que a criptografia pode e não pode fazer?

- A garantia de 100% de segurança é uma falácia, mas é possível trabalhar em direção a 100% de aceitação de riscos.

Um bom sistema criptográfico atinge o equilíbrio entre o que é possível e o que é aceitável."

"Existem homens de bom senso que, por serem incapazes de decifrar as coisas que são 'grego' para eles, convencem-se de que a lógica e a filosofia estão acima deles. Pois bem, gostaria que vissem que, assim como a natureza os dotou de olhos com os quais podem enxergar as obras dela, também lhes concedeu cérebros para penetrar e compreendê-las."



Galileu Galilei

CRIPTOGRAFIA - FUNDAMENTOS

- **Criptografia** - Conjunto de técnicas que permitem tornar "incompreensível" uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e a compreenda.
- **Criptoanálise** - do grego **kryptos + análysis (decomposição)** - ciência que estuda a decomposição do que está oculto ou a "**quebra**" do sistema criptográfico.
- **Criptologia** - Criptografia + Criptoanálise.

7

CRIPTOGRAFIA - FUNDAMENTOS

- **Pré-requisitos da Criptografia**
  - Teoria de Números
  - Matemática Discreta
  - Teoria da Informação
  - Teoria de Probabilidade
  - Complexidade Computacional
  - Processamento de Sinais

8

CRIPTOGRAFIA - TERMINOLOGIA

Termo	Descrição
Texto claro, simples (*plain text*) ou mensagem	**Mensagem original**
Cifração ou criptografia	**Processo de *"embaralhar"* a mensagem de forma a ocultar seu conteúdo de outrem**
Texto cifrado (*cipher text, Encrypted Text*) ou criptograma	**Mensagem cifrada**
Decifração ou descriptografia	**Processo inverso de recuperação da *mensagem* a partir do *criptograma***
Chave criptográfica	**Parâmetro de controle. Segredo por meio do qual a mensagem pode ser cifrada ou decifrada**

9

CRIPTOGRAFIA - TERMINOLOGIA

Termo	Descrição
Algoritmo criptográfico	**Transformação matemática - converte uma mensagem em claro em uma mensagem cifrada e vice-versa.**
Alice	**Origem - Cifra uma mensagem.**
Bob	**Destino - Decifra uma mensagem.**
Eva	**Intruso – tenta interceptar e decifrar a mensagem.**

Alice e Bob são personagens fictícios, mas são nomes sistematicamente utilizados pelos especialistas de criptografia. É mais colorido do que falar apenas no emissor e receptor, ou em A e B. Utiliza-se habitualmente uma terceira personagem, que costuma receber o nome de Eva (*Eve*) e que representa aquela que se põe à escuta - ou seja, aquela que "eavesdrop".

10

CRIPTOGRAFIA – HISTÓRICO

Fases da evolução da criptografia

- Criptografia manual
- Criptografia por máquinas
- Criptografia em rede

Historicamente quatro grupos de pessoas utilizaram e contribuíram para a arte da criptografia: os militares, os diplomatas, as pessoas que gostam de guardar memórias e os amantes.

11

CRIPTOGRAFIA – HISTÓRICO

Criptografia manual

- A criptografia era feita manualmente através de algum processo predeterminado.
- **Exemplos**:
  - Cifras Hebraicas
  - Bastão de Licurgo
  - Crivo de Erastótenes
  - Código de Políbio
  - Código de César

12

CRIPTOGRAFIA – HISTÓRICO

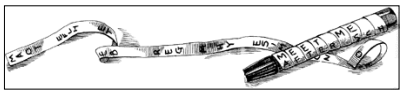
- **600 a 500 a.C.**
  - Escribas hebreus, no livro de Jeremias, usaram a cifra de substituição simples pelo alfabeto reverso - ATBASH. Cifras mais conhecidas da época: ATBASH, o ALBAM e o ATBAH – **cifras hebraicas**.
  - **ATBASH** - a primeira letra do alfabeto hebreu (Aleph) é trocada pela última (Taw), a segunda letra (Beth) e trocada pela penúltima (Shin) e assim sucessivamente. Destas quatro letras deriva o nome da cifra: **A**leph **T**aw **B**eth **SH**in - ATBASH.

Obs.: O barro de *Phaistos* (1600 a.c) ainda não decifrado.

13

CRIPTOGRAFIA – HISTÓRICO

- **487 a.C. - Bastão de Licurgo**
  - O remetente escreve a mensagem ao longo do bastão e depois desenrola a tira, a qual então se converte numa sequência de letras sem sentido. O mensageiro usa a tira como cinto, com as letras voltadas para dentro. O destinatário, ao receber o "cinto", enrola-o no seu bastão, cujo diâmetro é igual ao do bastão do remetente. Desta forma, pode ler a mensagem.



14

CRIPTOGRAFIA – HISTÓRICO

- **± 240 a.C - Crivo de Erastótenes**
  - Um dos meios mais eficientes de achar todos os números primos pequenos, por exemplo os menores que 10.000.000.
  - Basta fazer uma lista com todos os inteiros maiores que um e menores ou igual a *n* e riscar os múltiplos de todos os primos menores ou igual à raiz quadrada de *n* ($n^{1/2}$). **Os números que não estiverem riscados são os números primos**.
  - **Exemplo: Determinar os primos menores ou igual a 20**

(a)

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

(b)

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~

(c)

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~

(d)

	2	3	~~4~~	5	6	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~

CRIPTOGRAFIA – HISTÓRICO

± 150 a.C - Código de Políbio

- Cada letra é representada pela combinação de dois números, os quais se referem à posição ocupada pela letra. Desta forma, A é substituído por 11, B por 12...,
- A mensagem pode ser transmitida com dois grupos de 5 tochas. Por exemplo, a letra E é transformada em 1 e 5 e pode ser transmitida com 1 tocha à direita e 5 à esquerda.
- Um sistema de telecomunicação - um telégrafo ótico

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K/Q	L	M	N	O
4	P	R	S	T	U
5	V	W	X	Y	Z

16

CRIPTOGRAFIA – HISTÓRICO

50 a.C. - Código de César

- Cada letra da mensagem original é substituída pela letra que a seguia em três posições no alfabeto: a letra A substituída por D, a B por E, e assim até a última letra, cifrada com a primeira.
- Único da antiguidade usado até hoje, apesar de representar um retrocesso em relação à criptografia existente na época.
- **Denominação atual para qualquer cifra baseada na substituição cíclica do alfabeto: Código de César**.

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
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

17

CRIPTOGRAFIA – HISTÓRICO

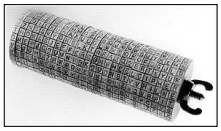
Criptografia por Máquinas

- Uma tabela predeterminada era usada em conjunto com uma máquina, em que o operador desta, usando a tabela e manipulando a máquina, podia enviar uma mensagem criptografada.
- **Exemplos de máquinas de criptografia**:
  - O Cilindro de Jefferson
  - O Código Morse
  - O Código Braille
  - O Código ASCII
  - A Máquina Enigma
  - A Máquina Colossus

18

CRIPTOGRAFIA – HISTÓRICO

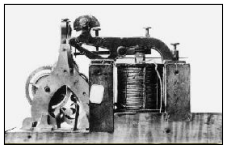
- **O cilindro de Jefferson (Thomas Jefferson, 1743-1826)**
  - Na sua forma original, é composto por 26 discos de madeira que giram livremente ao redor de um eixo central de metal.
  - As vinte e seis letras do alfabeto são inscritas aleatoriamente na superfície mais externa de cada disco de modo que, cada um deles, possua uma sequência diferente de letras.
  - Girando-se os discos pode-se obter as mensagens.



19

CRIPTOGRAFIA – HISTÓRICO

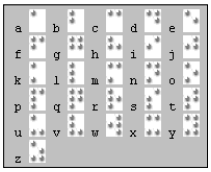
- **Samuel Morse (1791-1872)** desenvolve o código que recebeu o seu nome.
  - Na verdade não é um código, mas sim um alfabeto cifrado em sons curtos e longos.
  - Morse também foi o inventor do telégrafo.



20

CRIPTOGRAFIA – HISTÓRICO

- **Louis Braille (1809-1852)**
  - O **Código Braille** consiste de 63 caracteres, cada um deles constituído por 1 a 6 pontos dispostos numa matriz ou célula de seis posições.
  - O Sistema Braille é universalmente aceito e utilizado até os dias de hoje.

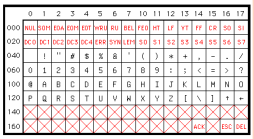


21

CRIPTOGRAFIA – HISTÓRICO

Código ASCII

- Gottfried Wilhelm von **Leibniz** (1646-1716) inventou o cálculo diferencial e integral, a máquina de calcular e descreveu minuciosamente o **sistema binário**.
- Sua máquina de calcular usava a escala binária. Esta escala, obviamente mais elaborada, é utilizada até hoje e é conhecida como código **ASCII** (*American Standard Code for Information Interchange)* - permitiu que máquinas de diferentes fabricantes trocassem dados entre si.



	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
000	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	FEO	HT	LF	VT	FF	CR	SO	SI
020	DC0	DC1	DC2	DC3	DC4	ERR	SYN	LETP	S0	S1	S2	S3	S4	S5	S6	S7
040		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
060	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
100	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
120	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	↑	←
140																
160													ACK		ESC	DEL

22

CRIPTOGRAFIA – HISTÓRICO

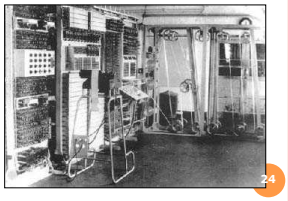
Máquina Enigma (1919)

- Máquina cifrante baseada em rotores.
- Foi um dos segredos mais bem guardados na Segunda Grande Guerra, usada pelos Alemães para proteger as comunicações entre o comando e as embarcações navais.
- **1940** (Alan Turing e sua equipe) – construção do primeiro computador operacional para o serviço de inteligência britânico - ***Heath Robinson.***
- ***Heath Robinson*** - utilizava tecnologia de relés e foi construído especificamente para decifrar mensagens alemãs (durante a Segunda Guerra Mundial) cifradas pela máquina ***Enigma***.

23

CRIPTOGRAFIA – HISTÓRICO

- **1943** – Os ingleses (Alan Turing) desenvolvem uma nova máquina para substituir o *Heath Robinson* – **Colossus.**



24

CRIPTOGRAFIA – HISTÓRICO

Criptografia em rede (computadores)

- A mensagem é criptografada usando-se algoritmos.
- Com o advento da internet e sua popularização, a criptografia em rede tem sido responsável pelo surgimento/fortalecimento do comércio eletrônico.
- **Exemplos**:
  - O DES (*Data Encryption Standard*), da IBM
  - O RSA (**R**onald Rivest, Adi **S**hamir e Leonard **A**dleman)
  - O PGP (*Pretty Good Privacy*), de Phil Zimmerman
  - outras codificações (nas telecomunicações: celulares, satélites, etc.)

25

CRIPTOGRAFIA - FUNDAMENTOS

Divisões da Criptografia

- Criptografia **fraca**
- Criptografia **forte**

26

CRIPTOGRAFIA - FUNDAMENTOS

Criptografia fraca

- Maneira banal de tentar ocultar informações de pessoas leigas no assunto.
- **Exemplo**: jogo criptograma - a pessoa deve chegar a identificar uma frase analisando certos símbolos.

27

CRIPTOGRAFIA - FUNDAMENTOS

- **Criptografia Forte**
  - De alta complexidade que visa manter as informações ocultas mesmo sob intensa verificação de supercomputadores.
  - Pode ser feita de duas formas:
    - em **chaves públicas** ou em **chaves privadas**.
  - **Exemplo**: PGP (*Pretty Good Privacy*).

Geralmente, a maneira mais fácil de determinar se um algoritmo é forte ou fraco consiste em publicar sua descrição, fazendo com que várias pessoas possam discutir sobre a eficiência ou não dos métodos utilizados.

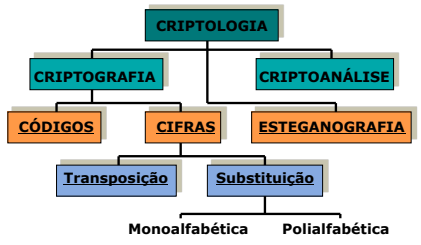
28

CRIPTOGRAFIA - FUNDAMENTOS

- **Chave pública** - a forma de criptografia é passada publicamente, para diversas pessoas, porém a maneira de descriptografá-las fica apenas com a pessoa/empresa que criou a chave.
- **Chave privada** - o criador é o único que sabe como codificar e decodificar, somente poderão ler ou esconder a informação aqueles a quem ele passar as instruções para fazê-lo.

29

CRIPTOGRAFIA - FUNDAMENTOS



30

Cifra considerada inviolável: Cifra (ou chave) de uso único (***one-time-pad***).

CRIPTOGRAFIA - FUNDAMENTOS

Formas de Criptografia

- **Por código** – procura esconder o conteúdo da mensagem por meio de códigos pré-definidos entre as partes envolvidas na troca de mensagens (substitui uma palavra por outra palavra ou símbolo)
- **Exemplo:** código utilizado pelas forças armadas dos EUA na 2ª Guerra Mundial. Utilizado pelos índios navajo que se comunicavam uns com os outros usando palavras navajo específicas para termos militares (exemplo: *chay-dagahi-nail-tsaidi* – assassino de cágado – indicar arma antitanque).

31

Parte da História dos índios navajo poderá ser vista no filme ***Códigos de Guerra***.

CRIPTOGRAFIA - FUNDAMENTOS

Formas de Criptografia

- **Por cifra** – o conteúdo da mensagem é cifrado por meio da mistura e/ou substituição das letras da mensagem original. Transformação de caractere por caractere (ou de bit por bit). Não considera a estrutura lingüística da mensagem. A mensagem é decifrada fazendo-se o processo inverso ao ciframento.
- **Exemplo**: Cifras Hebráicas
- **Tipos**:
  - **de Transposição** e
  - **de Substituição**.

32

CRIPTOGRAFIA – FUNDAMENTOS

- **Cifras de Transposição**: método pelo qual o conteúdo da mensagem é o mesmo, porém com as letras postas em ordem diferente (permutadas).
- **Exemplo**: pode-se cifrar a palavra *carro* e escrevê-la como ORARC.

33

CRIPTOGRAFIA – FUNDAMENTOS

Uma cifra de transposição

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Chave

Texto claro

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Texto cifrado

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Lido em colunas, a partir da coluna cuja letra da chave é a mais baixa (mais próxima do início do alfabeto).

Cifra de blocos de 64 caracteres.
Saída: 4, 12, 20, 28, 36, 44, 52, 60, 5, 13, ..., 62.

34

CRIPTOGRAFIA – FUNDAMENTOS

- **Cifras de Substituição**: troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição.
- **Tipos**:
  - **Cifra de substituição simples, monoalfabética ou Cifra de César**
  - **Cifra de substituição polialfabética**
  - **Cifra de substituição por deslocamento**

35

CRIPTOGRAFIA – FUNDAMENTOS

Cifra de substituição simples, monoalfabética

- **Texto cifrado** - substitui-se cada caractere do texto claro por outro, de acordo com uma tabela pré-estabelecida.
- Mantém a freqüência relativa dos caracteres.
- Criptografia contemporânea (uso de computadores) - substitui-se caracteres por blocos de bits.
- Relativamente segura em textos muito curtos. Uma simples criptanálise estatística, baseada na característica estatística da língua, é suficiente para decifrar o texto.

36

CRIPTOGRAFIA – FUNDAMENTOS

- **Cifra de substituição simples, monoalfabética**
  - **Monográmica** (monográfica) - cada letra da mensagem original é substituída por apenas uma outra letra, número ou símbolo.
  - O comprimento da mensagem cifrada é o mesmo da mensagem original.
  - **Exemplo**: Utilizando o Código de César, *ataque* é criptografado como DWDTXH.

37

CRIPTOGRAFIA – FUNDAMENTOS

- Cada símbolo (letra) é substituído por outro
  - por função matemática
  - por tabela
- Considerando 26 letras,
  - tem-se **26!** possibilidades (cerca de $4x10^{26}$)
  - Com 1 *ns* por tentativa, são **necessários ~10^{10}** anos para experimentar todas as chaves.

38

CRIPTOGRAFIA – FUNDAMENTOS

Cifra de deslocamento

- Geralização da cifra de César
- Cada c = (m + k) mod n
  - c : texto cifrado
  - m: texto claro
  - k: chave (deslocamento)
  - n: quantidade de símbolos ou letras
- Cifra de César
  c = (m + 3) mod 26

```
teste de uma cifra de cesar
whvwh gh xpd fliud gh fhvdu
```

39

CRIPTOGRAFIA – FUNDAMENTOS

Criptoanálise (Exemplo)

- Muito poucas tentativas (só 26)

```
alzal kl bth jpmyh kl klzsvjhtluzv
zkyzk jk asg iolxg jk jkyruigsktzu
yjxyj ij zrf hnkwf ij ijxqthfrjsyt
xiwxi hi yqe gmjve hi hiwpsgeqirxs
whvwh gh xpd fliud gh ghvorfdphqwr
vguvg fg woc ekhtc fg fgunqecogpvq
uftuf ef vnb djgsb ef eftmpdbnfoup
teste de uma cifra de deslocamento
```

40

CRIPTOGRAFIA – FUNDAMENTOS

- **Cifra de substituição simples, monoalfabética**
  - **Poligrâmica** (poligráfica) = vários caracteres.
  - Substitui um ou mais caracteres da mensagem original por uma ou mais letras, números ou símbolos.
  - Comprimento da mensagem cifrada nem sempre é o mesmo da mensagem original.
  - Substituição homofônica ("mesmo som") - sequências diferentes de letras pronunciadas de forma semelhante.
  - Traduz um único símbolo do texto claro para um de muitos símbolos cifrados, todos com o mesmo significado.
  - **Exemplo**: A cifra de Babou (substituir uma letra por um de vários símbolos), *aba* pode corresponder a MÃE e *abb* corresponder a JKL

41

CRIPTOGRAFIA – FUNDAMENTOS

- **Cifra de substituição simples, monoalfabética**
  - **Sistemas tomogrâmicos** - cada letra é representada por um grupo de duas ou mais letras ou números.
  - Estas letras ou números são obtidos através de uma cifragem por substituição ou por transposição separada.
  - **Exemplo**: O Código de Políbio.

42

CRIPTOGRAFIA – FUNDAMENTOS

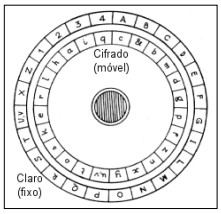
- **Cifra de substituição polialfabética**
  - **Substituição polialfabética** - utiliza múltiplos alfabetos para a substituição de uma mesma mensagem.
  - Os alfabetos não precisam necessariamente ser de origens diferentes. O simples fato de alterar a ordem na sequência das letras já caracteriza um "novo" alfabeto.
  - Dificulta a interpretação do texto cifrado pela aplicação da análise de frequência.
  - **Exemplo**: O Disco de Alberti.

43

CRIPTOGRAFIA – FUNDAMENTOS

- **Cifra de substituição polialfabética**

O Disco de Alberti



44

CRIPTOGRAFIA – FUNDAMENTOS

- **Cifra (ou chave) de uso único (*one-time-pad*)**
  - Cifra inviolável.
  - **Técnica**:
    1. Escolher como chave um string de bits aleatórios.
    2. Converter o texto simples em um string de bits (utilizando Código ASCII);
    3. Calcular o OR exclusivo (XOR) dos dois strings.
  - **Imune a ataques** – Teoria da Informação – não existe nenhuma informação na mensagem, todos os textos possíveis com o tamanho dado são igualmente prováveis.

45

CRIPTOGRAFIA – FUNDAMENTOS

Uso de uma chave única para criptografia e a possibilidade de conseguir texto simples que seja possível a partir do texto cifrado pela utilização de alguma outra chave.

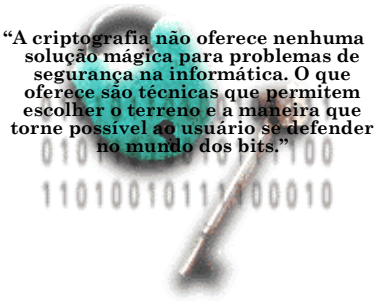
"I love you" convertida em ASCII de 7 bits

Operação XOR

Mensagem 1:	1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Chave 1:	1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Texto cifrado:	0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101
Chave 2:	1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Texto simples 2:	1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011

"Elvis lives" ?????

46



"A criptografia não oferece nenhuma solução mágica para problemas de segurança na informática. O que oferece são técnicas que permitem escolher o terreno e a maneira que torne possível ao usuário se defender no mundo dos bits."

47