

Tópicos Avançados em Computação I

Criptografia

“Ementa”

- Conceitos Introdutórios
- Tipos de ataques e cifras simétricas
- Estruturas tradicionais de cifras e DES
- Cifras modernas e seus modos de operação
- Funções de Hash Criptográficas
- Esquemas de Hash de Senhas
- Códigos de Autenticação de Mensagens
- Criptografia Assimétrica
- Assinaturas Digitais
- ...

Avaliação

- $NF = (TB + AV) / 2$

$$TB = 0.6 * EX + 0.4 * EP$$

AV = Avaliação Escrita

Repositiva substitui TB ou AV.

Referências

- Capítulo 01 - Introdução

William Stallings

CRIPTOGRAFIA e Segurança de redes PRINCÍPIOS E PRÁTICAS

6^a EDIÇÃO



Referências

- Capítulo 01
 - Introdução e Motivações

Routo Terada



To EDGAR A. POE, Esq.

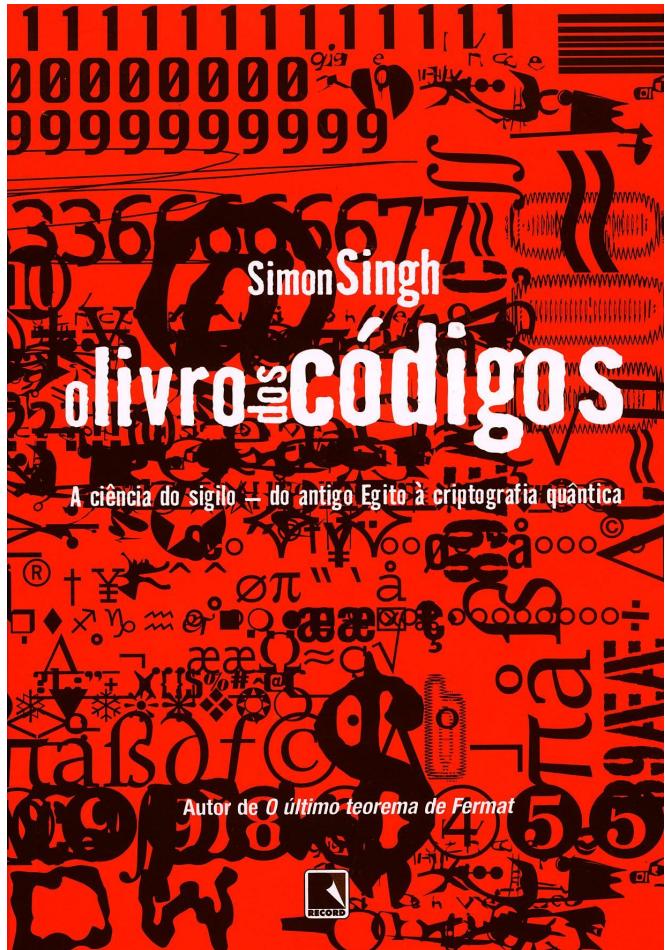
2^a EDIÇÃO
Revista e ampliada

Revista e ampliada

Blucher

Referências

- O código de Maria, rainha da Escócia



Tipos de ataques (*modelos genéricos*)



Taxonomia

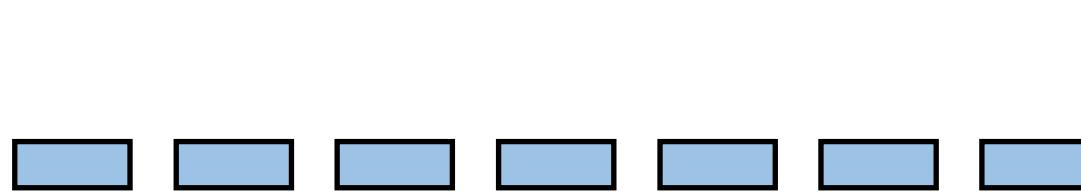
- Taxonomia baseada na fonte:
 - Ataques internos: usuários autorizados fazendo mau uso do sistema
 - Ataques externos: usuários não autorizados
- Taxonomia baseada no processo:
 - Ataques passivos
 - Ataques ativos

Qualquer um destes tipos de ataque irá alterar o fluxo normal da informação.

Taxonomia

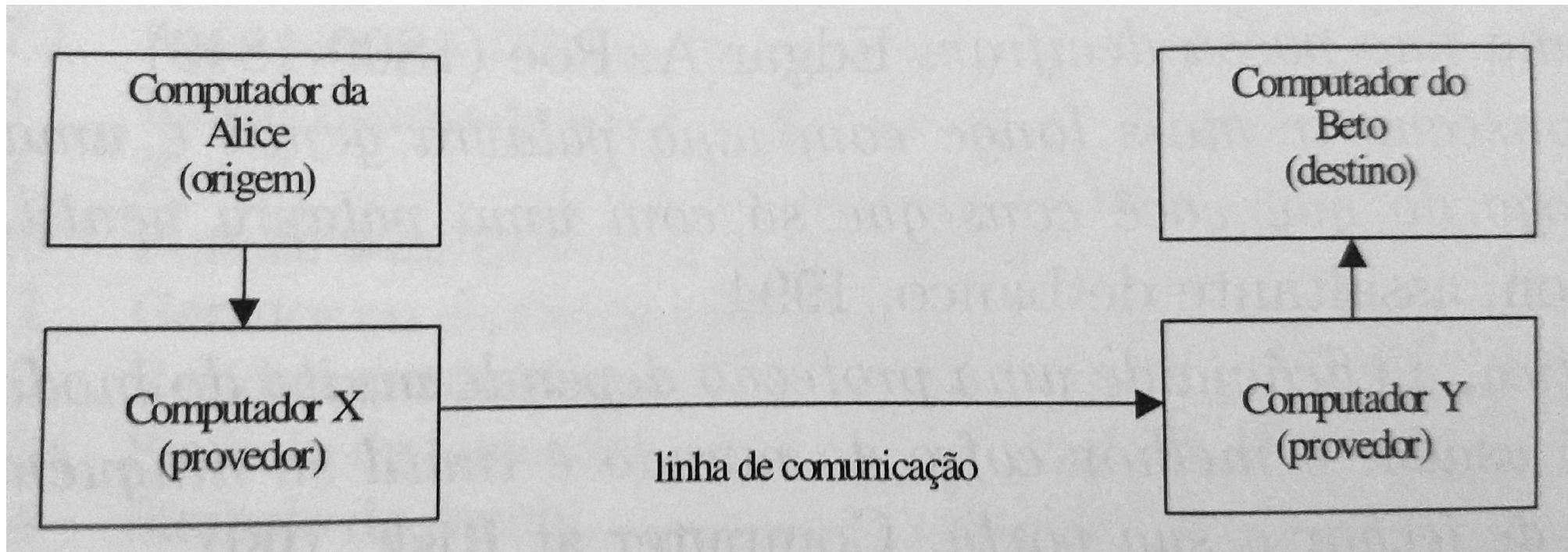


Origem



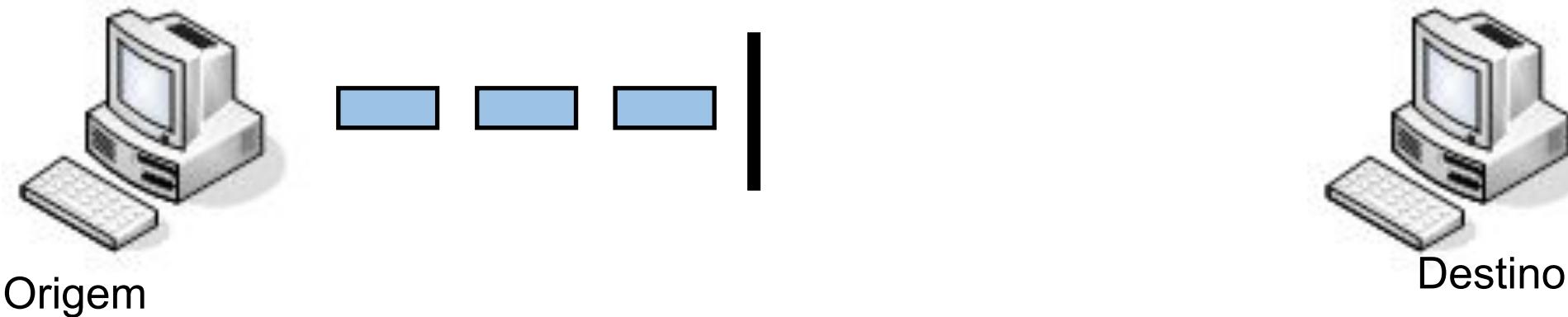
Destino

Taxonomia



Interrupção

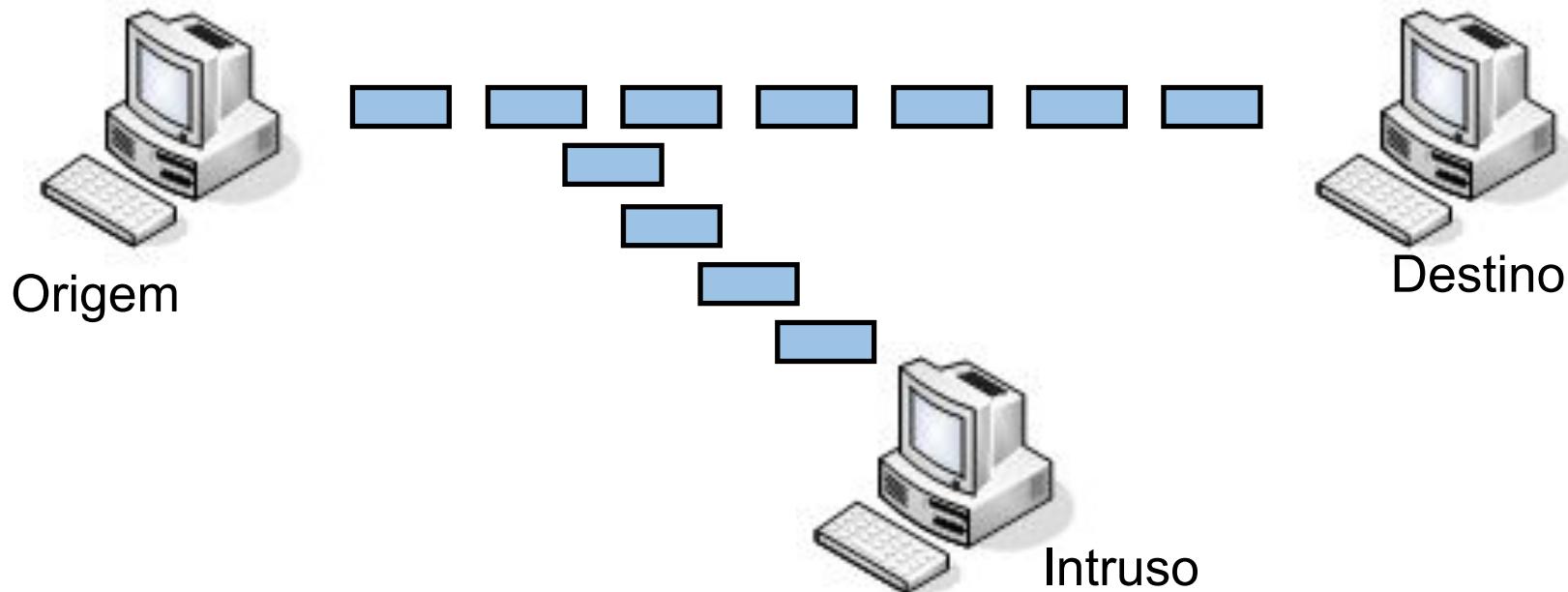
- Dados nunca chegam ao destino



- É necessária a segurança física dos recursos de processamento e de comunicação de dados! (*disponibilidade*)

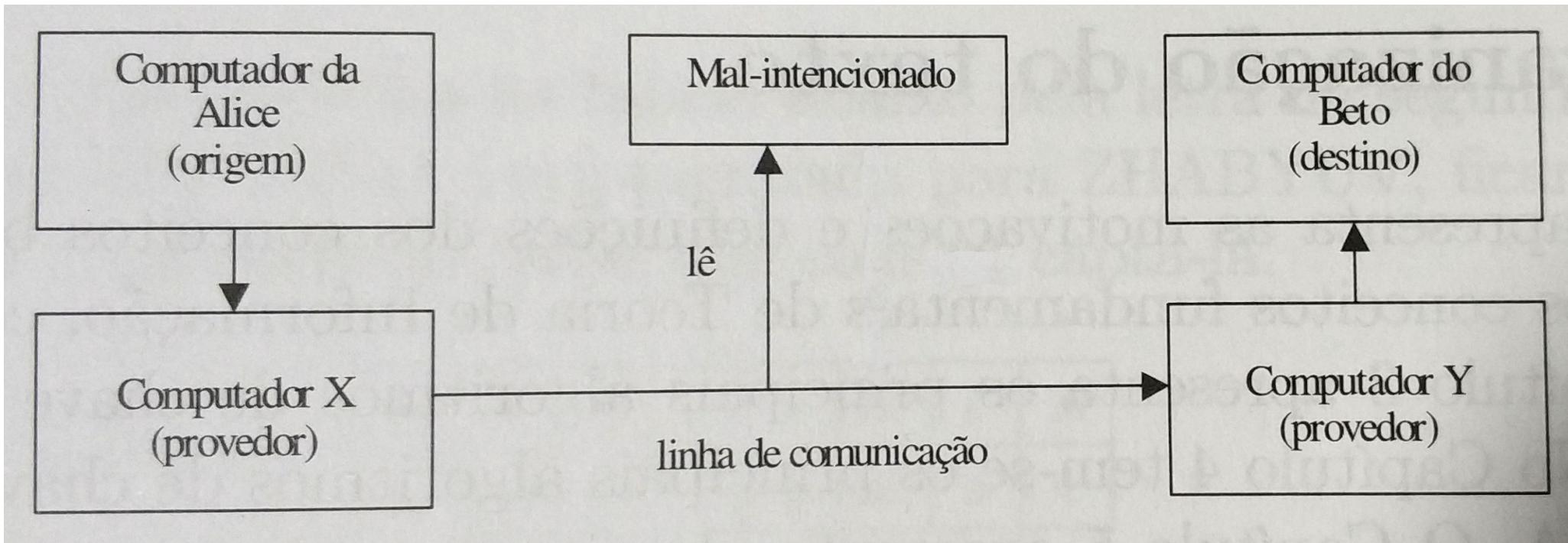
Interceptação

- Vazamento de informações !!!

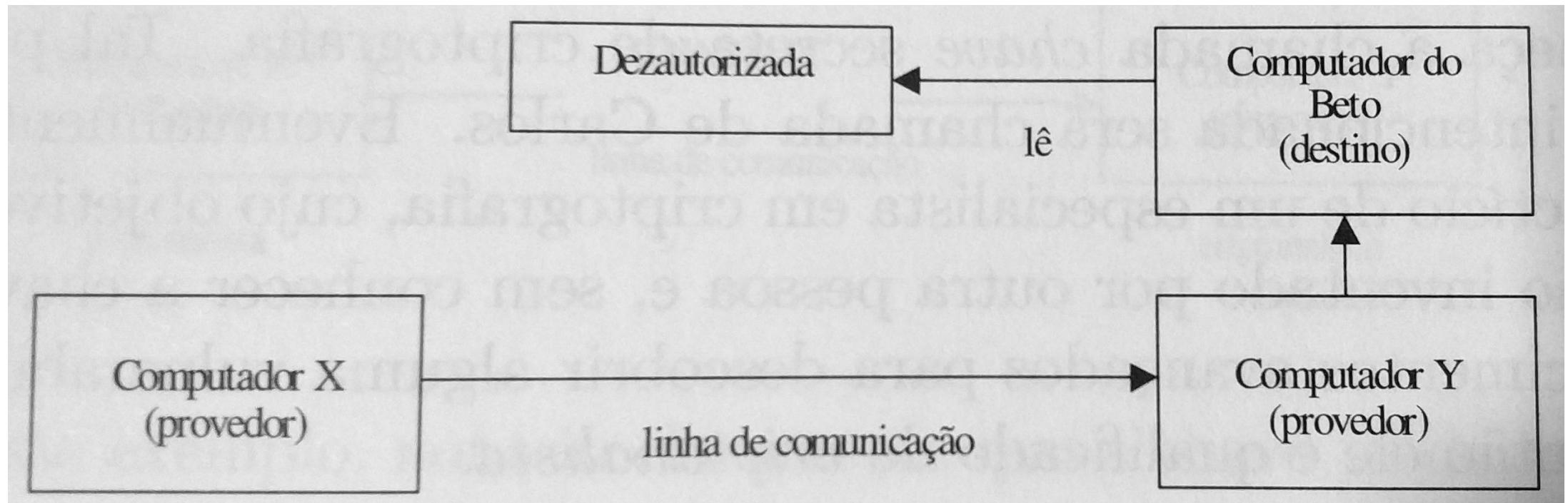


- Para evitar que o intruso entenda o conteúdo das mensagens, é necessário cifrar os dados (*confidencialidade*)

Interceptação

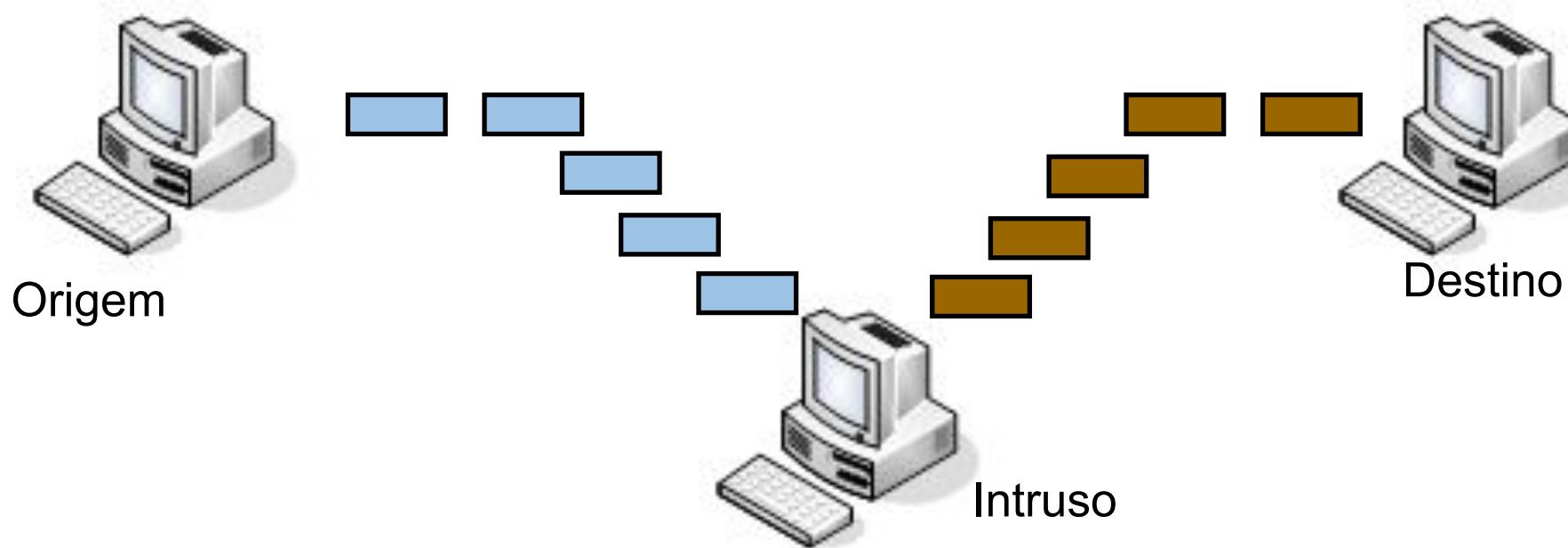


Interceptação



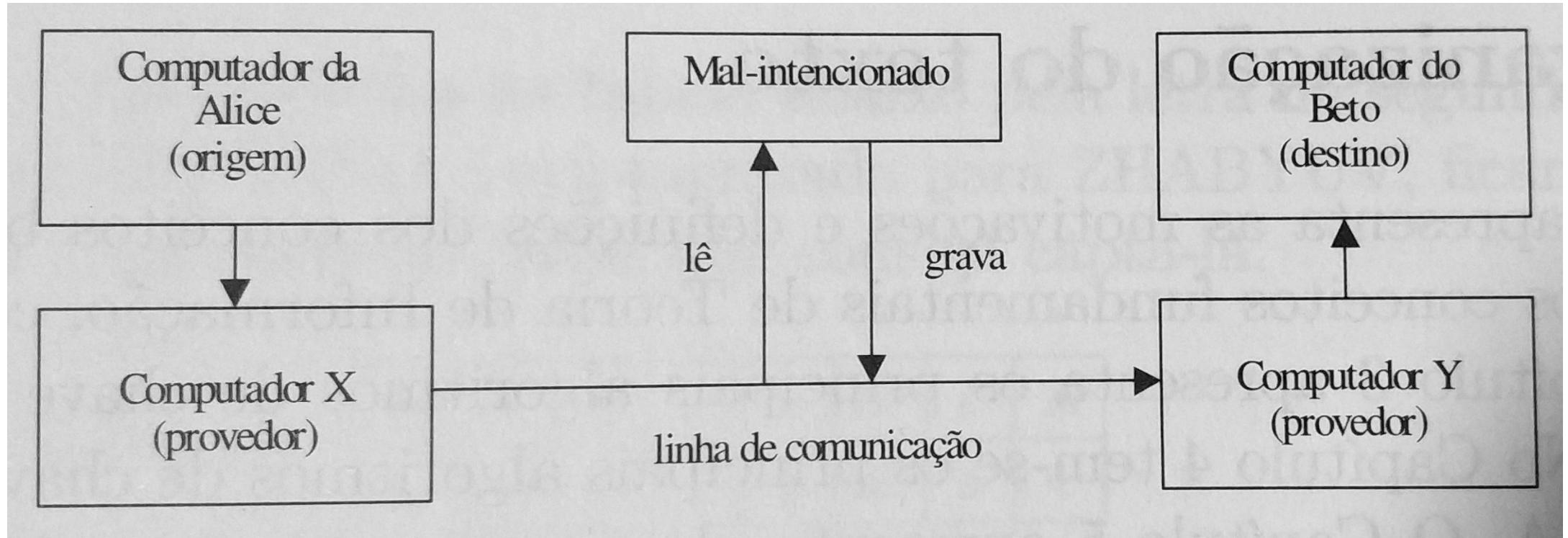
Modificação

- Informações Corrompidas/Falsas



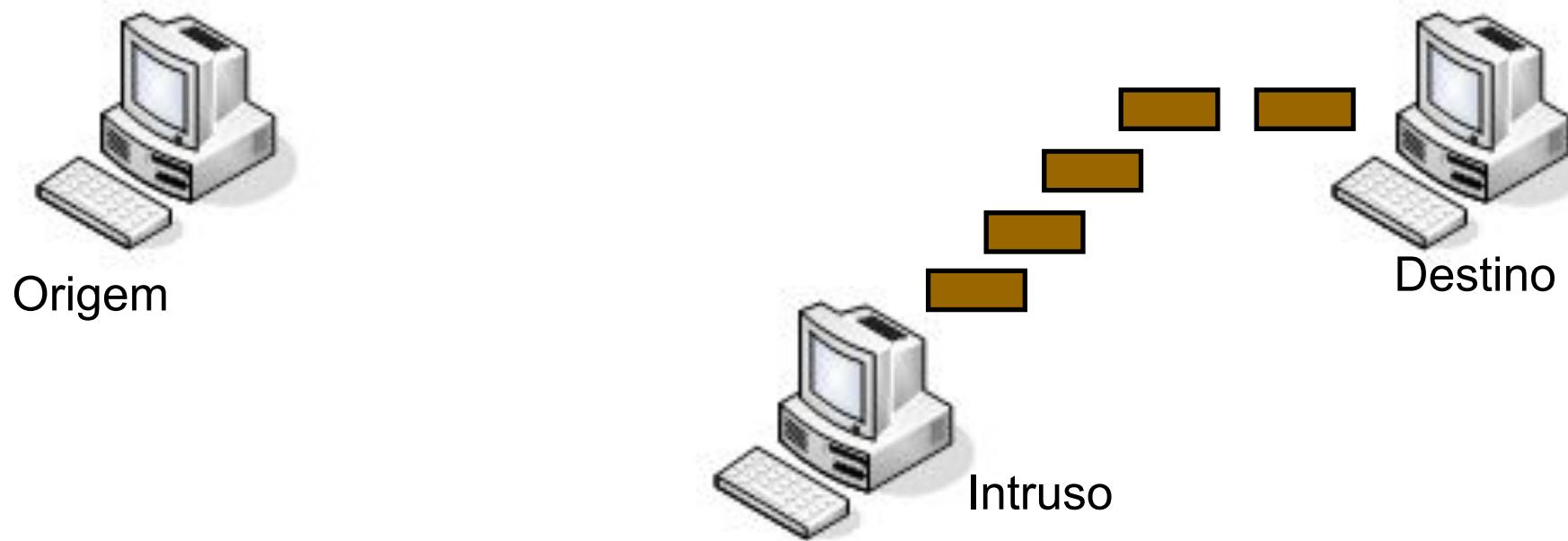
- Para evitar este tipo de ataque é preciso garantir a *integridade* e a *autenticidade* dos dados

Modificação



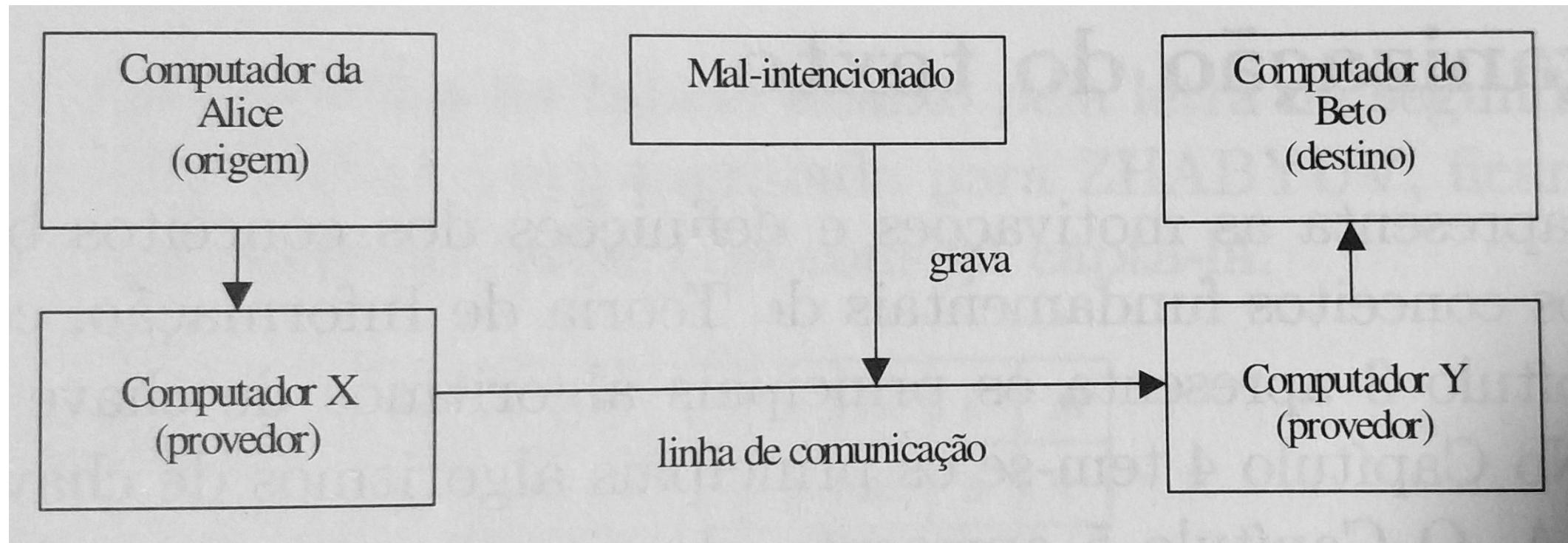
Fabricação

- Criação de informações que podem nunca terem existido

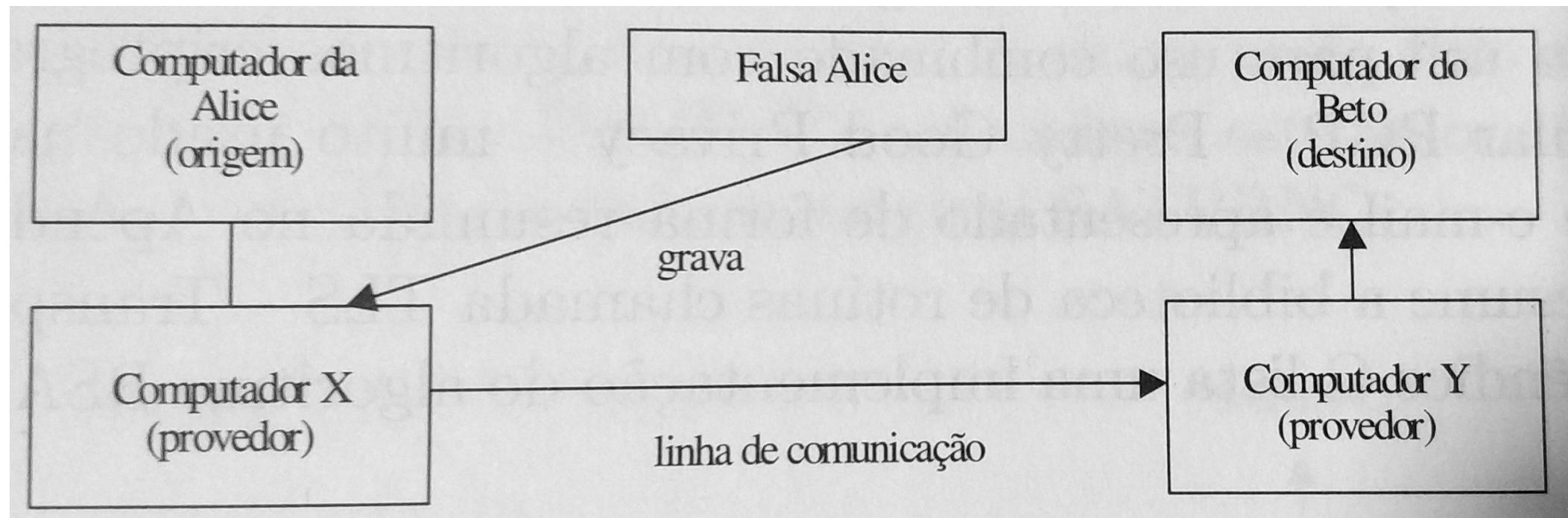


- Para evitar este tipo de ataque é preciso garantir a *autenticidade* dos dados

Fabricação



Fabricação



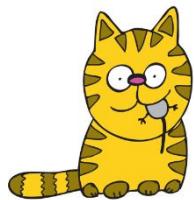
Outros ataques à confidencialidade

- **Inferência:** análise de dados permitem deduzir algo sobre a informação neles contida
- **Exposição:** dados fornecidos diretamente a entidade não autorizada (ex.: enviados para endereço de e-mail errado)
- **Intrusão:** atacante burla proteções do sistema e acessa dados

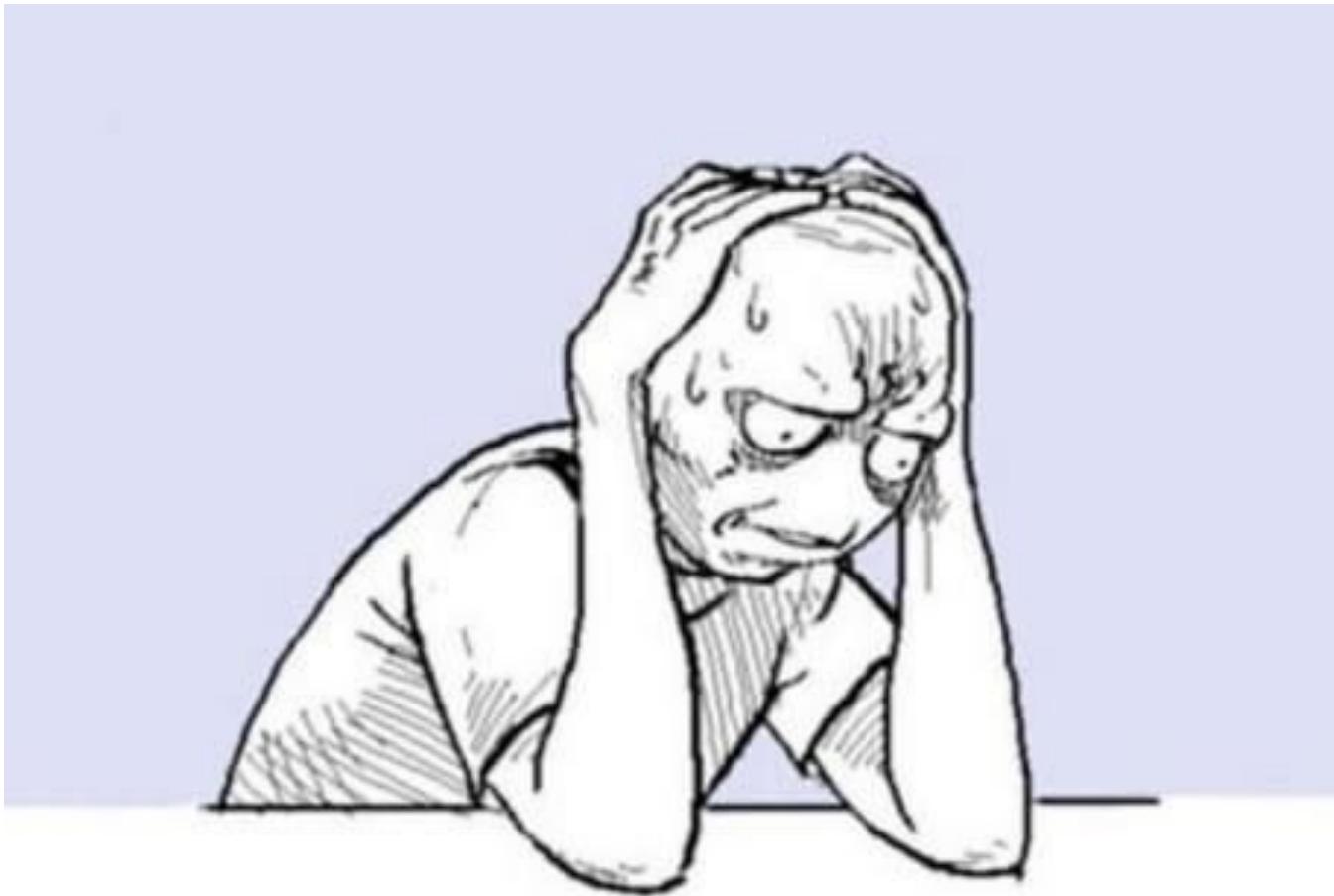


Outros ataques à confidencialidade

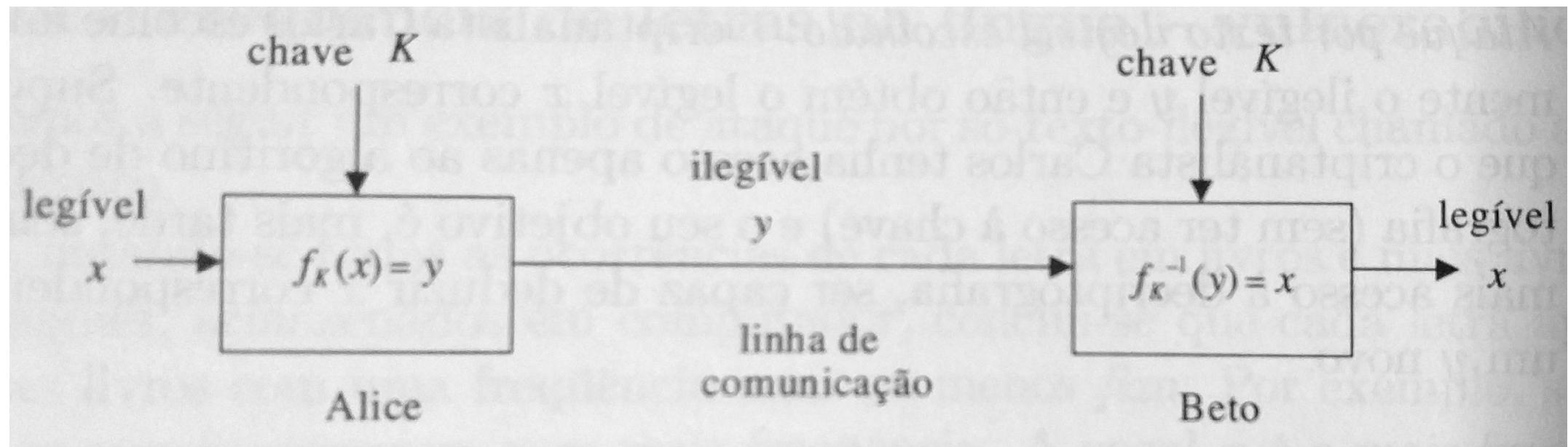
- **Personificação:** atacante se passa por uma entidade autorizada
 - Pode obter acesso a recursos do sistema: confidencialidade
 - Pode alterar recursos do sistema: integridade
 - Pode enviar mensagens falsas (fabricação): autenticidade
- **Retratação:** Uma entidade engana outra negando falsamente a responsabilidade por um ato
 - Irretratabilidade
 - E vários outros...



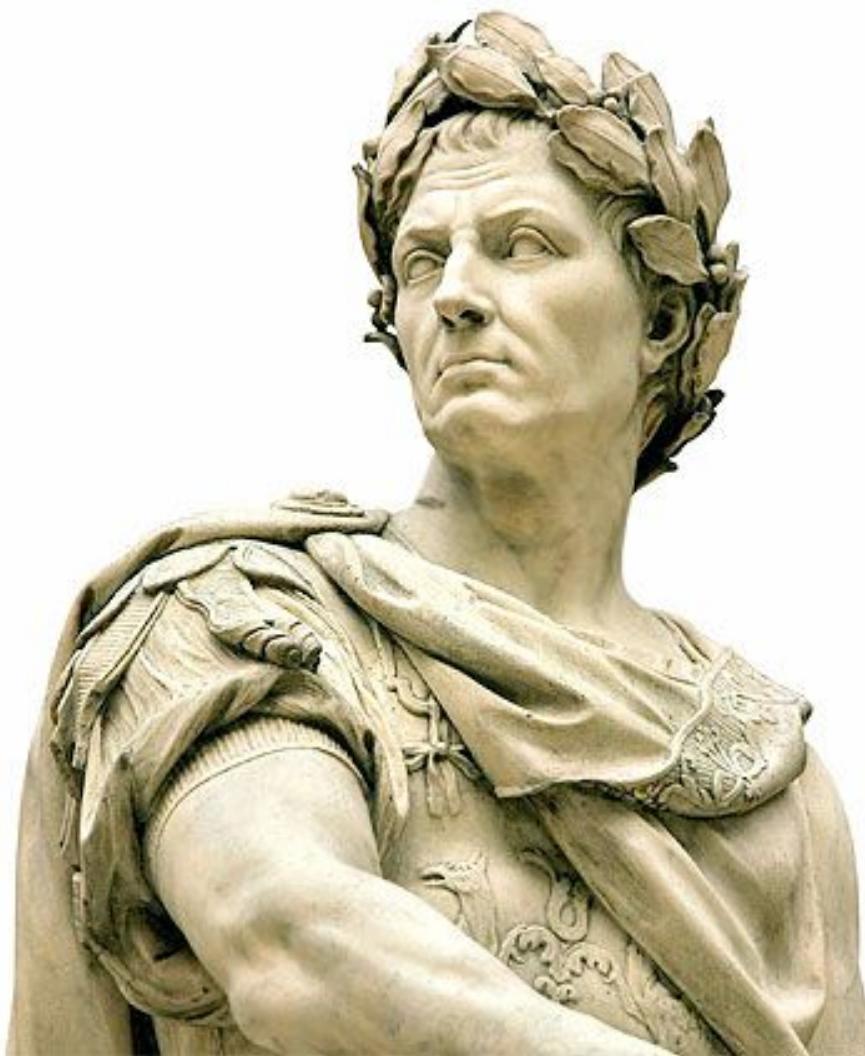
Como prover segurança?



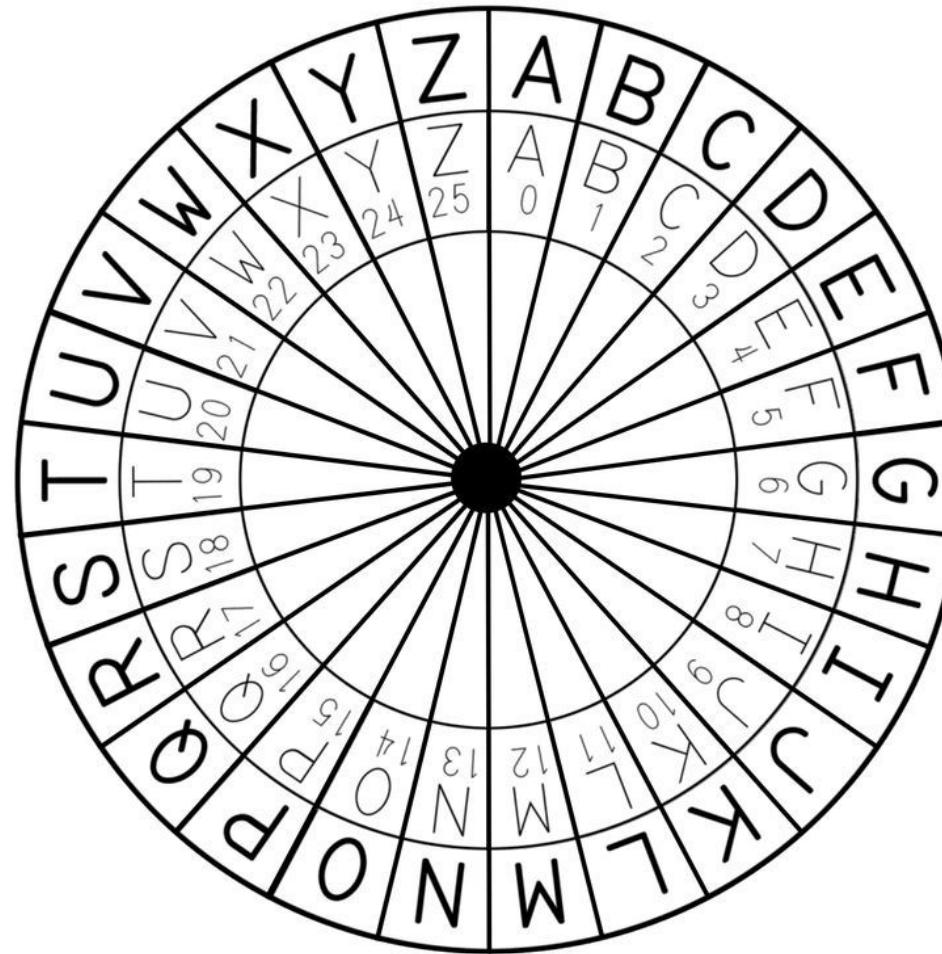
Criptografia



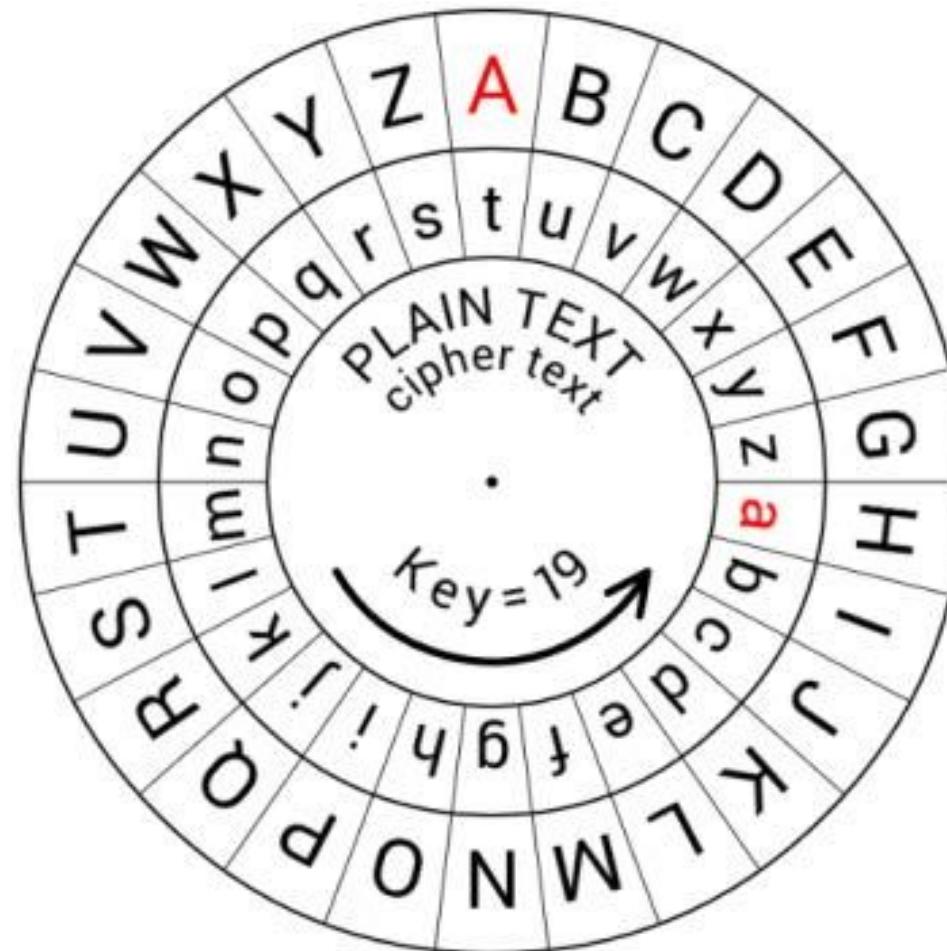
Cifra de César



Cifra de César



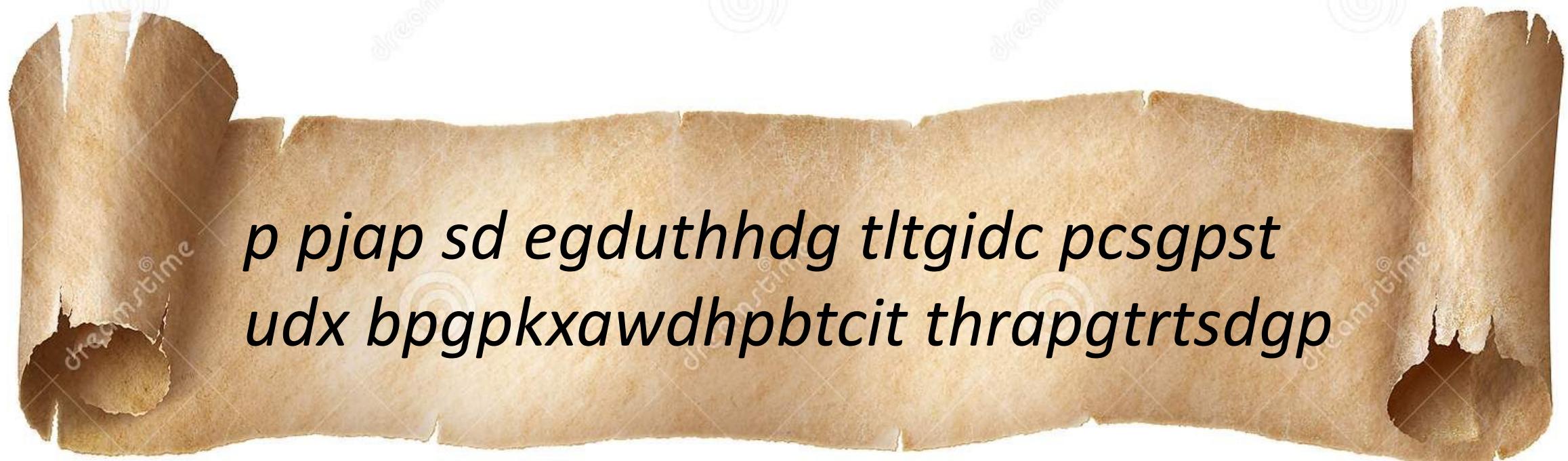
Cifra de César



Cifra de César



Cifra de César (*Mensagem cifrada*)



p pjap sd egduthhdg tltgidc pcsgpst
udx bpgpkxawdhpbtcit thrapgtrtsdgp

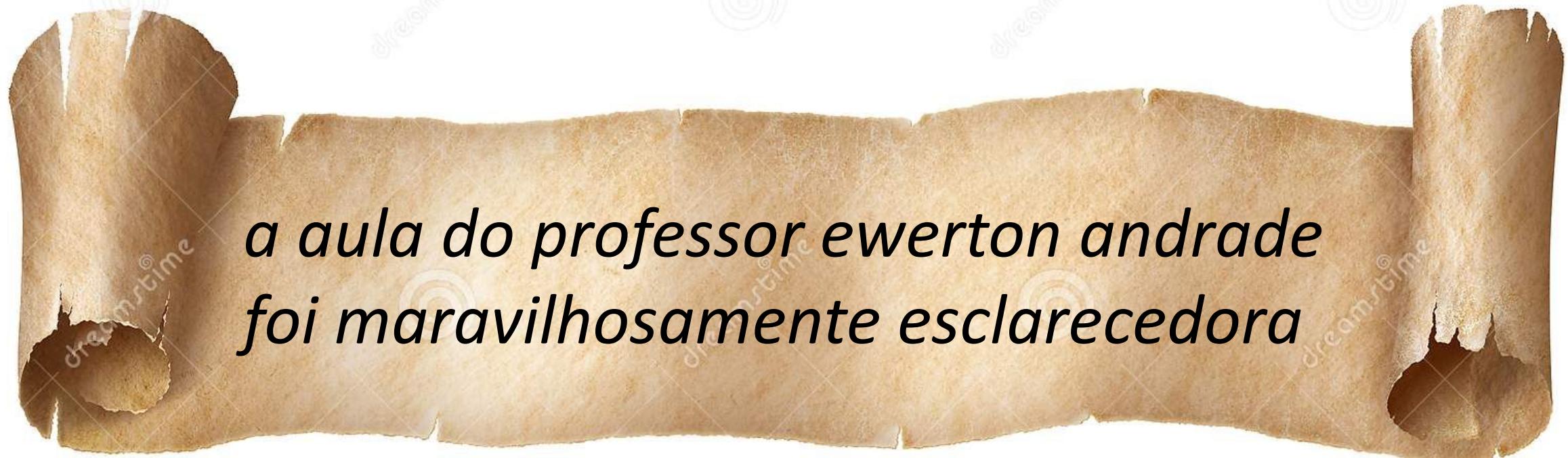
Cifra de César (*Mensagem cifrada*)



Aplicando a chave

“15”

Cifra de César (*Mensagem decifrada*)



*a aula do professor ewerton andrade
foi maravilhosamente esclarecedora*

Análise de frequência

- Análise de frequência é um método empregado para decifrar mensagens criptografadas por meio da análise, no texto criptografado, de padrões que se repetem constantemente, que podem indicar a ocorrência de letras ou de palavras de uso corriqueiro, tais como preposições ("de", "da"), pronomes, ("não", "sim"), etc.



Análise de frequência

[1] English Letter Frequency (based on a sample of 40,000 words). Disponível em:

<http://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html>

[2] Project Gutenberg. Disponível em:

http://www.gutenberg.org/wiki/Main_Page

[3] Simon Singh, Codici e Segreti, 1999, RCS, ISBN 88-17-12539-3.

Letra	Português	Inglês	Italiano
a	14.63%	8.17%	11.74%
b	1.04%	1.49%	0.92%
c	3.88%	2.78%	4.50%
d	4.99%	4.25%	3.73%
e	12.57%	12.70%	11.79%
f	1.02%	2.23%	0.95%
g	1.30%	2.02%	1.64%
h	1.28%	6.09%	1.54%
i	6.18%	6.97%	11.28%
j	0.40%	0.15%	0.00%
k	0.02%	0.77%	0.00%
l	2.78%	4.03%	6.51%
m	4.74%	2.41%	2.51%
n	5.05%	6.75%	6.88%
o	10.73%	7.51%	9.83%
p	2.52%	1.93%	3.05%
q	1.20%	0.10%	0.51%
r	6.53%	5.99%	6.37%
s	7.81%	6.33%	4.98%
t	4.34%	9.06%	5.62%
u	4.63%	2.76%	3.01%
v	1.67%	0.98%	2.10%
w	0.01%	2.36%	0.00%
x	0.21%	0.15%	0.00%
y	0.01%	1.97%	0.00%
z	0.47%	0.07%	0.49%

Tabela 1. Tabela de frequências em diferentes idiomas.

Referências (*material de apoio*)

- Uma jornada pela criptografia

<https://pt.khanacademy.org/computing/computer-science/cryptography>



Cifra de Vigenère (*Polialfabética*)

	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	V
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	W
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	X
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



Perguntas para revisão

- 1) Quais são os elementos essenciais de uma cifra simétrica?
- 2) Quantas chaves são necessárias para duas pessoas se comunicarem por meio de uma cifra simétrica?
- 3) O número total de chaves possíveis na Cifra de César corresponde ao tamanho do alfabeto (i.e., n , onde n é o tamanho do alfabeto). Sendo assim, qual o número total de chaves possíveis na Cifra de Vigenère?
- 4) O que é um algoritmo seguro?



Exercício de Programação 01

Elabore um programa que possa realizar um ataque de frequência na primeira palavra de um texto cifrado com a Cifra de César.

Seu software deverá:

- receber o texto cifrado
- receber a palavra conhecida
- calcular e exibir a chave de decifragem



Exercício de Programação 02

Elabore um programa que implemente a Cifra de Vigenère (Polialfabética).



Obrigado!

ewerton.andrade@unir.br

<http://ewerton.andrade.pro.br/>

