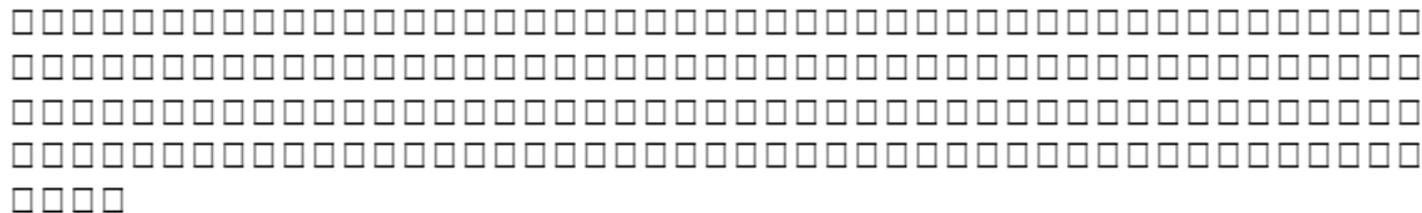


# Aspectos de Segurança em Automação

OUTRAS AULAS EM:

[www.projetederedes.com.br](http://www.projetederedes.com.br)

José Maurício S. Pinheiro - UBM - 2016



A forma mais utilizada para prover a segurança em pontos vulneráveis de uma rede de computadores é a utilização da criptografia. A criptografia é utilizada para barrar as ameaças e os ataques.

A forma mais utilizada para prover a segurança em pontos vulneráveis de uma rede de computadores é a utilização da criptografia. A criptografia é utilizada para barrar as ameaças e os ataques.

# Definindo Criptografia

- A RFC 2828 (*Request for Comments* nº 2828) define o termo criptografia como a ciência matemática que lida com a transformação de dados para mudar seu significado em algo ininteligível.
- O objetivo é esconder o conteúdo semântico da mensagem prevenindo sua alteração ou o seu uso sem autorização.

# Métodos de Criptografia

- **Cifra de substituição** - cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, afim de ocultá-la.
- **Cifra de transposição** - as letras são reordenadas mas não ocultadas. A cifra é chaveada por uma palavra ou frase que não contém quaisquer letras repetidas.

# Exemplo de Criptografia por cifra

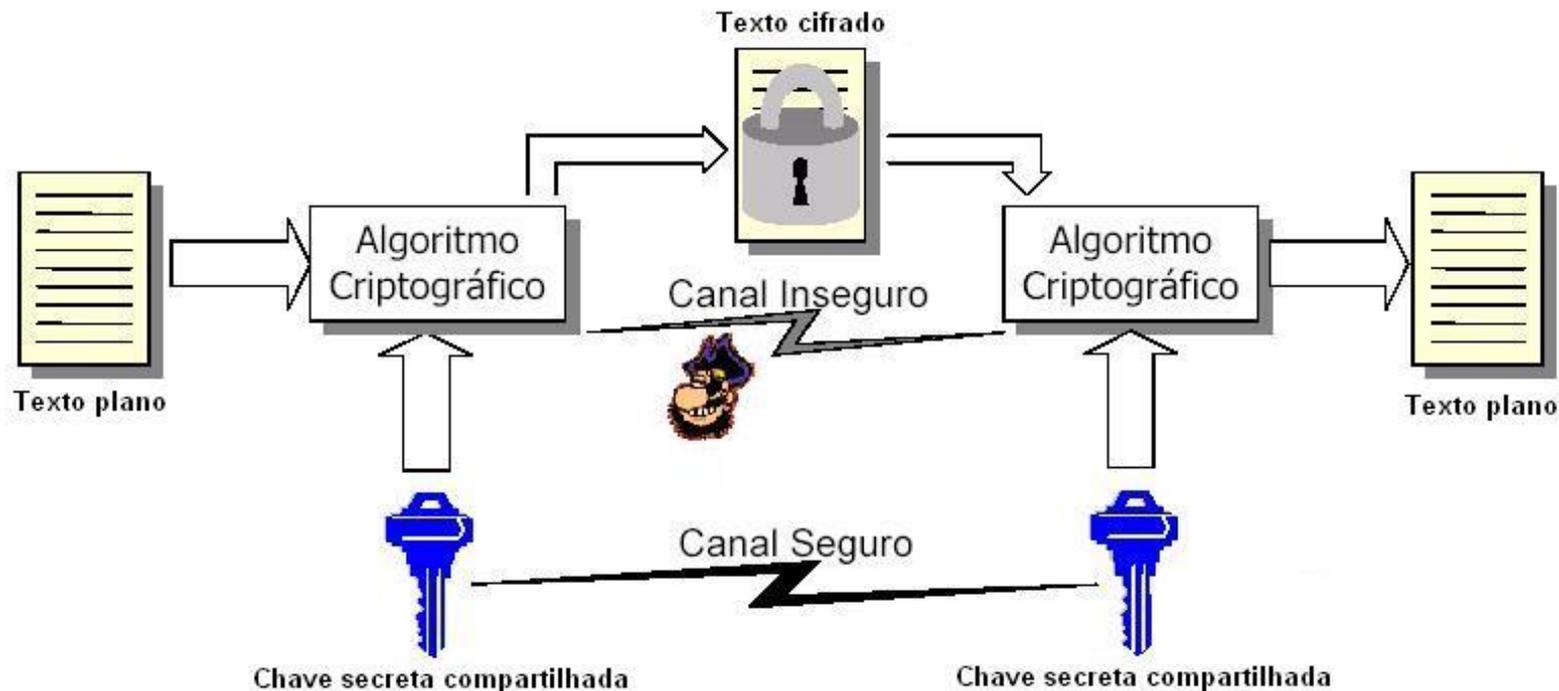
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

- EXEMPLIFIQUE
- EXEMPLIFIQUE  $\Rightarrow$  XEMELPFIQIEU (inverte cada 2 letras)
- A A A A A A | B A A A A A  
A B C D E F | B C D E F G (deslocamento pela letra ant.)

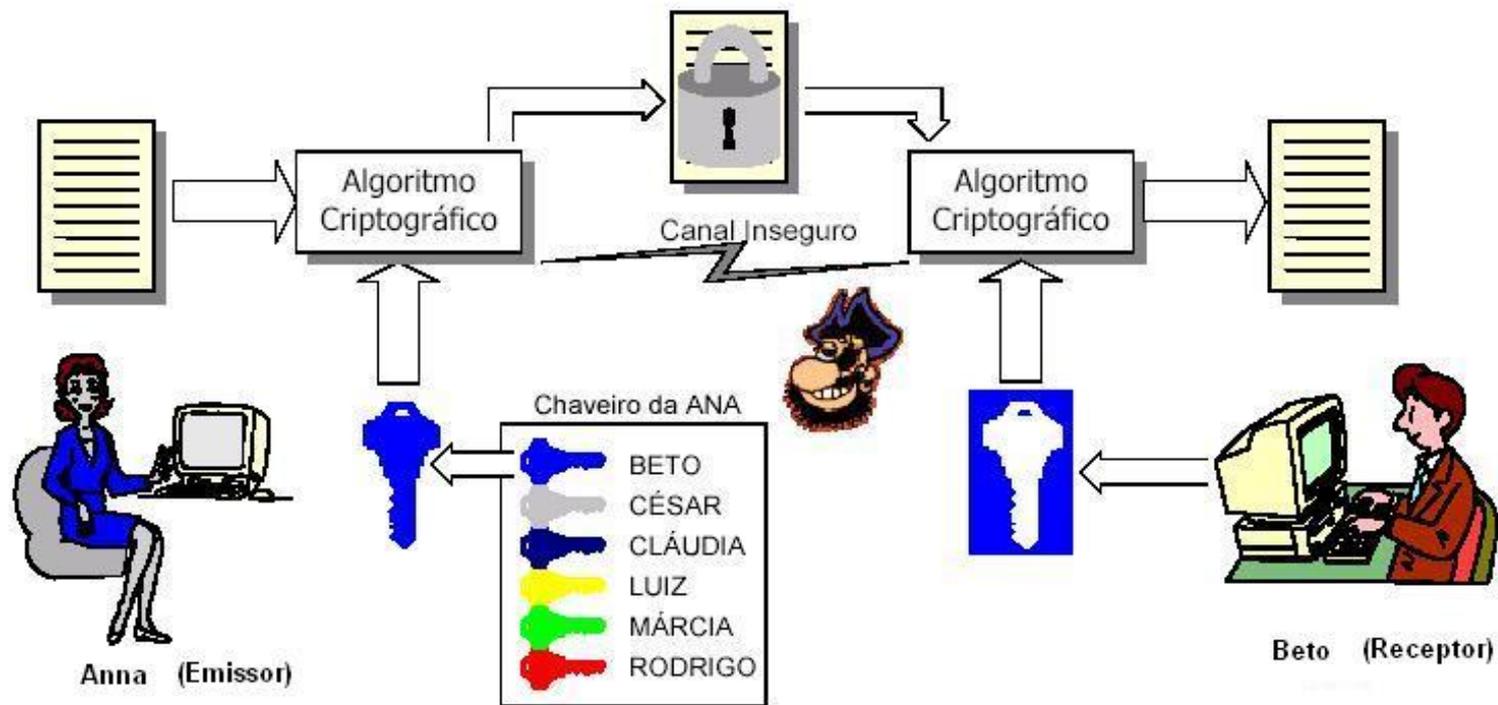
# Tempos de Busca

Tamanho da Chave	Número de Chaves	Tempo requerido (1 cripto/ $\mu$ s)	Tempo requerido ( $10^6$ cripto/ $\mu$ s)
32	$2^{32} = 4,3 \times 10^9$	35,8 minutos	2,15 ms
56	$2^{56} = 7,2 \times 10^{16}$	1.142 anos	10,01 horas
128	$2^{128} = 3,4 \times 10^{38}$	$5,4 \times 10^{24}$ anos	$5,4 \times 10^{18}$ anos
26 caracteres (permutação)	$26! = 4 \times 10^{26}$	$6,4 \times 10^{12}$ anos	$6,4 \times 10^6$ anos

# Criptografia Simétrica ou de Chave Privada



# Criptografia Assimétrica ou de Chave Pública



# Características dos Algoritmos

<b>CHAVE PRIVADA</b>	<b>CHAVE PÚBLICA</b>
Um algoritmo e uma chave	Um algoritmo e duas chaves
Os usuários compartilham o algoritmo e a chave	Os usuários compartilham um par de chaves
Chave secreta	Apenas uma das chaves é secreta
Impossibilidade de decifrar a mensagem	Impossibilidade de decifrar a mensagem
O algoritmo e as amostras do texto cifrado não devem ser suficientes para determinar a chave	O algoritmo, as amostras do texto cifrado e uma das chaves não devem ser suficientes para determinar a outra chave

# Definindo Esteganografia

Ramo particular da criptografia que consiste, não em fazer com que uma mensagem seja ininteligível, mas em camuflá-la, mascarando a sua presença.

# Métodos de Esteganografia

- **Marcação de caracteres:** utilização de uma tinta com composto diferente que ao ser colocada frente à luz faz com que os caracteres fiquem de forma diferente, compondo a mensagem secreta;
- **Tinta invisível:** pode-se utilizar uma tinta invisível para a escrita da mensagem em cima de outra pré-existente, aonde, somente com produtos químicos poderíamos obter o conteúdo.
- **Bits não significativos:** Utiliza o uso de bits não significativos que são concatenados a mensagem original e faz uso também de área não usada.

Autenticação ou assinatura digital é a versão digital da assinatura de punho em documentos físicos.

O destinatário de uma mensagem assinada digitalmente pode verificar se a mensagem foi realmente emitida pela pessoa cuja assinatura nela consta, ou se a mensagem foi adulterada intencional ou acidentalmente depois de assinada.