

Usando criptografia de forma prática e descomplicada

Marcos Azevedo aka psylinux

BSidesSP - Edição 0xF - Maio 2018

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❶ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❶ Criptografia Assimétrica
 - ❶ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❶ Assinatura de Arquivo
 - ❶ Criptografia de Arquivos
 - ❶ Assinatura de E-mail
 - ❶ Criptografia em E-mail
 - ❶ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - Cifra de César
- ❹ Introdução à criptografia
 - Definições e terminologias
 - Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - Definições e terminologias
 - Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ➊ Apresentação Pessoal
- ➋ Qual a relevância desse tema?
- ➌ História da Criptografia
 - ➊ Cifra de César
- ➍ Introdução à criptografia
 - ➊ Definições e terminologias
 - ➋ Visão geral e funcionamento básico
- ➎ Alguns tipos de criptografia
 - ➊ Criptografia Simétrica
 - ➋ Criptografia Assimétrica
 - ➌ Assinatura Digital
- ➏ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ➊ GPG e PGP
 - ➋ Assinatura de Arquivo
 - ➌ Criptografia de Arquivos
 - ➍ Assinatura de E-mail
 - ➎ Criptografia em E-mail
 - ➏ Chave GPG para Login em SSH
- ➐ Considerações finais

- ➊ Apresentação Pessoal
- ➋ Qual a relevância desse tema?
- ➌ História da Criptografia
 - ➊ Cifra de César
- ➍ Introdução à criptografia
 - ➊ Definições e terminologias
 - ➋ Visão geral e funcionamento básico
- ➎ Alguns tipos de criptografia
 - ➊ Criptografia Simétrica
 - ➋ Criptografia Assimétrica
 - ➌ Assinatura Digital
- ➏ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ➊ GPG e PGP
 - ➋ Assinatura de Arquivo
 - ➌ Criptografia de Arquivos
 - ➍ Assinatura de E-mail
 - ➎ Criptografia em E-mail
 - ➏ Chave GPG para Login em SSH
- ➐ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

- ❶ Apresentação Pessoal
- ❷ Qual a relevância desse tema?
- ❸ História da Criptografia
 - ❶ Cifra de César
- ❹ Introdução à criptografia
 - ❶ Definições e terminologias
 - ❷ Visão geral e funcionamento básico
- ❺ Alguns tipos de criptografia
 - ❶ Criptografia Simétrica
 - ❷ Criptografia Assimétrica
 - ❸ Assinatura Digital
- ❻ Ferramentas para usar no dia-a-dia (Linux e Windows)
 - ❶ GPG e PGP
 - ❷ Assinatura de Arquivo
 - ❸ Criptografia de Arquivos
 - ❹ Assinatura de E-mail
 - ❺ Criptografia em E-mail
 - ❻ Chave GPG para Login em SSH
- ❼ Considerações finais

Marcos Azevedo - Consultor de Segurança na Cipher. Possui mais de 15 anos de experiência em Segurança da Informação, onde os últimos quatro anos foram dedicados a hardening de servidores, correção de problemas de segurança, análise forense, pentesting e segurança ofensiva. Ele tem um bom conhecimento de sistemas operacionais, arquitetura de computadores, compiladores e montadores para Intel x86, linguagem C, Python, PowerShell Scripts e Shell Scripts. Possui um sólido conhecimento de protocolos TCP/IP e experiência em infraestrutura de rede (Cisco Routers and Switches). Sua curva de aprendizado é muito rápida graças aos seus conhecimentos sólidos dos princípios da computação, além da motivação por desafios. Marcos já palestrou em conferências tais como: H2HC, FLISOL, FGSL e outros.

Figura: Goiânia, Goiás



Goianês ou Criptografia?

- **Dinheiro pra sapecar porco:** Muito dinheiro.
- **Custoso (a):** Difícil, pessoa sapeca.
- **Demais da conta:** Muito, muito mesmo.
- **Encabulado:** Impressionado.
- **Pizêro:** Bagunça.
- **Pulá o corguim:** Passar dos limites.
- **Apiar:** Descer.

Goianês ou Criptografia?

- **Dinheiro pra sapecar porco:** Muito dinheiro.
- **Custoso (a):** Difícil, pessoa sapeca.
- **Demais da conta:** Muito, muito mesmo.
- **Encabulado:** Impressionado.
- **Pizêro:** Bagunça.
- **Pulá o corguim:** Passar dos limites.
- **Apiar:** Descer.

Goianês ou Criptografia?

- **Dinheiro pra sapecar porco:** Muito dinheiro.
- **Custoso (a):** Difícil, pessoa sapeca.
- **Demais da conta:** Muito, muito mesmo.
- **Encabulado:** Impressionado.
- **Pizêro:** Bagunça.
- **Pulá o corguim:** Passar dos limites.
- **Apiar:** Descer.

Goianês ou Criptografia?

- **Dinheiro pra sapecar porco:** Muito dinheiro.
- **Custoso (a):** Difícil, pessoa sapeca.
- **Demais da conta:** Muito, muito mesmo.
- **Encabulado:** Impressionado.
- **Pizêro:** Bagunça.
- **Pulá o corguim:** Passar dos limites.
- **Apiar:** Descer.

Goianês ou Criptografia?

- **Dinheiro pra sapecar porco:** Muito dinheiro.
- **Custoso (a):** Difícil, pessoa sapeca.
- **Demais da conta:** Muito, muito mesmo.
- **Encabulado:** Impressionado.
- **Pizêro:** Bagunça.
- **Pulá o corguim:** Passar dos limites.
- **Apiar:** Descer.

Goianês ou Criptografia?

- **Dinheiro pra sapecar porco:** Muito dinheiro.
- **Custoso (a):** Difícil, pessoa sapeca.
- **Demais da conta:** Muito, muito mesmo.
- **Encabulado:** Impressionado.
- **Pizêro:** Bagunça.
- **Pulá o corguim:** Passar dos limites.
- **Apiar:** Descer.

Goianês ou Criptografia?

- **Dinheiro pra sapecar porco:** Muito dinheiro.
- **Custoso (a):** Difícil, pessoa sapeca.
- **Demais da conta:** Muito, muito mesmo.
- **Encabulado:** Impressionado.
- **Pizêro:** Bagunça.
- **Pulá o corguim:** Passar dos limites.
- **Apiar:** Descer.

O que é Criptografia?

Visão Geral



"Criptografia"

Qual a relevância desse tema?

Qual a relevância desse tema?

Por que usamos criptografia?

Quando queremos que apenas o **EMISSOR** e o **DESTINATÁRIO** compreendam o conteúdo da mensagem.

Qual a relevância desse tema?

Quando usamos criptografia?

- **"Em trânsito"**, neste contexto, é quando você envia informações através da Internet, por e-mail ou quando precisa armazená-la em outro lugar que não seja o seu próprio dispositivo.
- **"Em repouso"**, quando estão armazenados em seu dispositivo, que pode ser parte integrada como um disco rígido, ou em um meio removível, como uma unidade USB.

Qual a relevância desse tema?

Quando usamos criptografia?

- "**Em trânsito**", neste contexto, é quando você envia informações através da Internet, por e-mail ou quando precisa armazená-la em outro lugar que não seja o seu próprio dispositivo.
- "**Em repouso**", quando estão armazenados em seu dispositivo, que pode ser parte integrada como um disco rígido, ou em um meio removível, como uma unidade USB.

- 1 **Criptografia Clássica:** Sustenta-se em leis matemáticas.
- 2 **Criptografia Quântica:** Utiliza-se de elementos físicos, tal com fótons, para gerar chaves quânticas inquebráveis.

- 1 **Criptografia Clássica:** Sustenta-se em leis matemáticas.
- 2 **Criptografia Quântica:** Utiliza-se de elementos físicos, tal com fótons, para gerar chaves quânticas inquebráveis.

- 1 **Algoritmo de transposição:** rearranja a ordem dos caracteres de uma mensagem. Um exemplo simples é a transformação de “**muito obrigado**” em “**omtui oobdraig**”. Esta categoria de algoritmo criptográfico é composta por uma função bijetora para efetuar encriptações e sua inversa faz a mensagem voltar à forma original;
- 2 **Algoritmo de substituição:** substitui caracteres ou grupos de caracteres por outros caracteres ou grupos de caracteres. Um exemplo simples: “**muito obrigado**” é transformado em “**nvjup pcsjhbeq**”, substituindo cada letra pela próxima na sequência alfabética.

- 1 **Algoritmo de transposição:** rearranja a ordem dos caracteres de uma mensagem. Um exemplo simples é a transformação de “**muito obrigado**” em “**omtui oobdraig**”. Esta categoria de algoritmo criptográfico é composta por uma função bijetora para efetuar encriptações e sua inversa faz a mensagem voltar à forma original;
- 2 **Algoritmo de substituição:** substitui caracteres ou grupos de caracteres por outros caracteres ou grupos de caracteres. Um exemplo simples: “**muito obrigado**” é transformado em “**nvjup pcsjhbeq**”, substituindo cada letra pela próxima na sequência alfabética.

Entendendo o Algoritmo de Euclides

O Algoritmo de Euclides nos fornece a seguinte propriedade: na k -ésima iteração, vale que

$$r_{k+1} = r_{k-1} - r_k q_k$$

em que $q_k = \frac{r_{k-1}}{r_k}$ é uma divisão inteira.

O algoritmo acaba quando $r_{k+1} = 0$, definindo o resto atual como o máximo divisor comum: $r_k = MDC(a, b)$.

Para estender o algoritmo, queremos também manter a seguinte propriedade:

$$r_k = au_k + bv_k$$

dessa forma, quando o algoritmo acabar, teremos valores u_k e v_k que satisfazem o [teorema de Bézout](#).

Para isso, assumamos que nós temos esses valores para a iteração k e para a iteração anterior, $k-1$: ou seja, assumamos que já temos os valores que satisfazem as duas igualdades a seguir:

$$r_k = au_k + bv_k$$

e

$$r_{k-1} = au_{k-1} + bv_{k-1}$$

então, para o próximo resto, teremos

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k \\ &= (au_{k-1} + bv_{k-1}) - (au_k + bv_k)q_k \\ &= au_{k-1} - au_k q_k + bv_{k-1} - bv_k q_k \\ &= a(u_{k-1} - u_k q_k) + b(v_{k-1} - v_k q_k) \\ &= au_{k+1} + bv_{k+1} \end{aligned}$$

Ou seja, se a igualdade de Bézout vale para a iteração atual do algoritmo e para a iteração anterior, então, ela vale para a próxima e os valores de Bézout são

$$u_{k+1} = u_{k-1} - u_k q_k$$

e

$$v_{k+1} = v_{k-1} - v_k q_k$$

BRINCADEIRA GENTE!

Mensagem: **CRIPTOGRAFIA NA BSIDES SAO PAULO 2018**

Criptografia Clássica

Algoritmo de Transposição

	1	2	3	4	5	6	7	8
1	C	R	I	P	T	O	G	R
2	A	F	I	A	N	A	B	S
3	I	D	E	S	S	A	O	P
4	A	U	L	O	2	0	1	8

Chave criptográfica: **24176835**

Criptografia Clássica

Algoritmo de Transposição

	1	2	3	4	5	6	7	8
1	I	C	G	R	R	T	P	O
2	I	A	B	F	S	N	A	A
3	E	I	O	D	P	S	S	A
4	L	A	1	U	8	2	O	0

Criptografia Clássica

Algoritmo de Substituição

3M UM D14 D3 VER40, 3S7AVA N4 PR4I4, O853RV4NDO DU4S
CR14NÇ4S 8B1NC4ND0 N4 4REI4. EL45 TR4B4LH4V4M MUI7O
C0N57R1ND0 UM C4ATEL0 D3 AR3I4, C0M 70RR35, P4554R3L4S
3 P4554G3N5 1N7ERN4S. QU4ND0 ES74V4M QU4S3 T3RM1N4ND0,
V310 UM4 0ND4 3 3S7RU1U 7UDO, R3DU21ND0 0 C4S7EL0
4 UM MON73 D3 4REI4 3 3SPUM4. 4CH31 QU3 D3P01S D3
74N70 35FORÇ0 3 CU1D4D0, 45 CR1ANC4S C4IR4M N0 CH0R0,
CORR3R4M P3L4 PR41A, FUG1ND0 DA 4GU4, R1ND0 D3 M405
D4D4S 3 C0M3C4R4M 4 C0NS7RU1R 0UTR0 C4573LO.

Algumas Aplicações da Criptografia Atualmente

- 1 Sigilo em banco de dados;
- 2 Censos;
- 3 Investigações governamentais;
- 4 Dossiês de pessoas sob investigação;
- 5 Dados hospitalares;
- 6 Informações de crédito pessoal;
- 7 Decisões estratégicas empresariais;
- 8 Sigilo em comunicação de dados;
- 9 Comandos militares;
- 10 Mensagens diplomáticas;
- 11 Operações bancárias;
- 12 Comércio eletrônico;
- 13 Transações por troca de documentos eletrônicos (EDI);
- 14 Estudo de idiomas desconhecidos;
- 15 Recuperação de documentos arqueológicos, hieróglifos;
- 16 E até tentativas de comunicações extraterrestres.

Introdução à Criptografia

Definições e terminologias — Criptologia

Criptologia: disciplina que reúne os conhecimentos e as técnicas necessários à criptoanálise ('solução de criptogramas') e à criptografia ('modificação codificada').

Introdução à Criptografia

Definições e terminologias — Texto Claro

Texto Claro: Texto original, não cifrado.

Introdução à Criptografia

Definições e terminologias — Texto Cifrado

Texto Cifrado: Texto ilegível, não compreensível.

Introdução à Criptografia

Definições e terminologias — Simetria

Simetria: conformidade, em medida, forma e posição relativa, entre as partes dispostas em cada lado de uma linha divisória, um plano médio, um centro ou um eixo

Assimetria: 1. ausência de simetria. 2. grande diferença; disparidade, discrepância

Introdução à Criptografia

Definições e terminologias — Encriptar/Cifrar

Encriptar/Cifrar: 1. reproduzir (mensagem) em código não conhecido, tornando-a, desse modo, intencionalmente ininteligível para os que não têm acesso às suas convenções. 2. inf codificar (informação) de modo que somente destinatários autorizados possam ter acesso a ela; encriptar.

Introdução à Criptografia

Definições e terminologias — Decriptar/Decifrar

Decriptar/Decifrar: traduzir ou decifrar mensagens ou códigos cifrados ou criptografados

Introdução à Criptografia

Definições e terminologias — Bit

Bit: menor parcela de informação processada por um computador.
Algarismo do sistema binário que somente pode assumir as formas 0 ou 1

Algoritmo: 1. mat sequência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas. 2. inf conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas.

O Princípio de Kerckhoff

O Princípio de Kerckhoff é um princípio fundamental na criptografia moderna:

”Um sistema de criptografia deve ser seguro mesmo se o adversário conhecer todos os detalhes do sistema, com exceção da chave secreta.”

- 1 **Cifradores de blocos:** divide a mensagem em blocos de tamanho fixo (ex: 256 bits). Por exemplo, DES, AES, 3DES
- 2 **Cifradores de fluxo:** cifra cada dígito do texto plano por vez. Por exemplo, o RC4

- 1 **Cifradores de blocos:** divide a mensagem em blocos de tamanho fixo (ex: 256 bits). Por exemplo, DES, AES, 3DES
- 2 **Cifradores de fluxo:** cifra cada dígito do texto plano por vez. Por exemplo, o RC4

Alguns tipos de Chaves Criptograficas

- 1 Criptografia Simétrica
- 2 Criptografia Assimétrica

Alguns tipos de Chaves Criptograficas

- 1 Criptografia Simétrica
- 2 Criptografia Assimétrica

Criptografia Simétrica

- 1 Também conhecido como: criptografia de chave única, criptografia de chave secreta.
- 2 A chave precisa ser transmitida através de um canal seguro.
- 3 Transmissão Wireless utilizam esse modelo criptográfico.

Criptografia Simétrica

- 1 Também conhecido como: criptografia de chave única, criptografia de chave secreta.
- 2 A chave precisa ser transmitida através de um canal seguro.
- 3 Transmissão Wireless utilizam esse modelo criptográfico.

Criptografia Simétrica

- 1 Também conhecido como: criptografia de chave única, criptografia de chave secreta.
- 2 A chave precisa ser transmitida através de um canal seguro.
- 3 Transmissão Wireless utilizam esse modelo criptográfico.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

- ❶ Baseado no par de chaves: **pública e privada**
 - Chaves públicas são divulgadas abertamente.
 - Chaves privadas devem ser mantidas em segredo.
 - Não é possível obter a chave privada a partir da pública!
- ❷ Provê:
 - Confidencialidade das mensagens.
 - Autenticação do remetente.
 - Verificação de integridade.
 - Não repúdio.

Ferramentas para usar no dia-a-dia (Linux e Windows)

- 1 GPG e PGP
- 2 Assinatura de Arquivo
- 3 Criptografia de Arquivos
- 4 Assinatura de E-mail
- 5 Criptografia em E-mail
- 6 Chave GPG para Login em SSH

Ferramentas para usar no dia-a-dia (Linux e Windows)

- 1 GPG e PGP
- 2 Assinatura de Arquivo
- 3 Criptografia de Arquivos
- 4 Assinatura de E-mail
- 5 Criptografia em E-mail
- 6 Chave GPG para Login em SSH

Ferramentas para usar no dia-a-dia (Linux e Windows)

- 1 GPG e PGP
- 2 Assinatura de Arquivo
- 3 Criptografia de Arquivos
- 4 Assinatura de E-mail
- 5 Criptografia em E-mail
- 6 Chave GPG para Login em SSH

Ferramentas para usar no dia-a-dia (Linux e Windows)

- 1 GPG e PGP
- 2 Assinatura de Arquivo
- 3 Criptografia de Arquivos
- 4 Assinatura de E-mail
- 5 Criptografia em E-mail
- 6 Chave GPG para Login em SSH

Ferramentas para usar no dia-a-dia (Linux e Windows)

- 1 GPG e PGP
- 2 Assinatura de Arquivo
- 3 Criptografia de Arquivos
- 4 Assinatura de E-mail
- 5 Criptografia em E-mail
- 6 Chave GPG para Login em SSH

Ferramentas para usar no dia-a-dia (Linux e Windows)

- 1 GPG e PGP
- 2 Assinatura de Arquivo
- 3 Criptografia de Arquivos
- 4 Assinatura de E-mail
- 5 Criptografia em E-mail
- 6 Chave GPG para Login em SSH

- ❶ Nunca, jamais, desenvolva o seu próprio algoritmo de criptografia, a menos que você tenha uma equipe de experientes criptoanalistas verificando o seu projeto.
- ❷ Não utilize algoritmos de criptografia não comprovados ou protocolos não comprovados.
- ❸ Os atacantes vão sempre olhar para o ponto mais fraco de um sistema de criptografia. Por exemplo, um grande espaço de chaves por si só não é garantia de uma cifra segura; a cifra ainda pode estar vulnerável contra ataques analíticos.

- ❶ Nunca, jamais, desenvolva o seu próprio algoritmo de criptografia, a menos que você tenha uma equipe de experientes criptoanalistas verificando o seu projeto.
- ❷ Não utilize algoritmos de criptografia não comprovados ou protocolos não comprovados.
- ❸ Os atacantes vão sempre olhar para o ponto mais fraco de um sistema de criptografia. Por exemplo, um grande espaço de chaves por si só não é garantia de uma cifra segura; a cifra ainda pode estar vulnerável contra ataques analíticos.

- ❶ Nunca, jamais, desenvolva o seu próprio algoritmo de criptografia, a menos que você tenha uma equipe de experientes criptoanalistas verificando o seu projeto.
- ❷ Não utilize algoritmos de criptografia não comprovados ou protocolos não comprovados.
- ❸ Os atacantes vão sempre olhar para o ponto mais fraco de um sistema de criptografia. Por exemplo, um grande espaço de chaves por si só não é garantia de uma cifra segura; a cifra ainda pode estar vulnerável contra ataques analíticos.

- 4 Comprimentos de chave de algoritmos simétricos, a fim de frustrar ataques de busca exaustiva da chave:
 - 64 bits: inseguro exceto para dados cujo uso se dará num prazo muito curto.
 - 128 bits: segurança de longo prazo para várias décadas, a menos que os computadores quânticos se tornem disponíveis (computadores quânticos não existem e talvez nunca existam).
 - 256 bits: como acima, mas provavelmente seguros até contra ataques por computadores quânticos.
 - Aritmética modular é uma ferramenta para exprimir os esquemas de encriptação históricos, tais como a Cifra Afim, de uma maneira matematicamente elegante.

- ④ Comprimentos de chave de algoritmos simétricos, a fim de frustrar ataques de busca exaustiva da chave:
 - 64 bits: inseguro exceto para dados cujo uso se dará num prazo muito curto.
 - 128 bits: segurança de longo prazo para várias décadas, a menos que os computadores quânticos se tornem disponíveis (computadores quânticos não existem e talvez nunca existam).
 - 256 bits: como acima, mas provavelmente seguros até contra ataques por computadores quânticos.
 - Aritmética modular é uma ferramenta para exprimir os esquemas de encriptação históricos, tais como a Cifra Afim, de uma maneira matematicamente elegante.

- ④ Comprimentos de chave de algoritmos simétricos, a fim de frustrar ataques de busca exaustiva da chave:
 - 64 bits: inseguro exceto para dados cujo uso se dará num prazo muito curto.
 - 128 bits: segurança de longo prazo para várias décadas, a menos que os computadores quânticos se tornem disponíveis (computadores quânticos não existem e talvez nunca existam).
 - 256 bits: como acima, mas provavelmente seguros até contra ataques por computadores quânticos.
 - Aritmética modular é uma ferramenta para exprimir os esquemas de encriptação históricos, tais como a Cifra Afim, de uma maneira matematicamente elegante.

- ④ Comprimentos de chave de algoritmos simétricos, a fim de frustrar ataques de busca exaustiva da chave:
 - 64 bits: inseguro exceto para dados cujo uso se dará num prazo muito curto.
 - 128 bits: segurança de longo prazo para várias décadas, a menos que os computadores quânticos se tornem disponíveis (computadores quânticos não existem e talvez nunca existam).
 - 256 bits: como acima, mas provavelmente seguros até contra ataques por computadores quânticos.
 - Aritmética modular é uma ferramenta para exprimir os esquemas de encriptação históricos, tais como a Cifra Afim, de uma maneira matematicamente elegante.

- ④ Comprimentos de chave de algoritmos simétricos, a fim de frustrar ataques de busca exaustiva da chave:
 - 64 bits: inseguro exceto para dados cujo uso se dará num prazo muito curto.
 - 128 bits: segurança de longo prazo para várias décadas, a menos que os computadores quânticos se tornem disponíveis (computadores quânticos não existem e talvez nunca existam).
 - 256 bits: como acima, mas provavelmente seguros até contra ataques por computadores quânticos.
 - Aritmética modular é uma ferramenta para exprimir os esquemas de encriptação históricos, tais como a Cifra Afim, de uma maneira matematicamente elegante.

Considerações Finais