Oficina de Criptografia

Técinas para segurança e privacidade na computação

Coletivo Encripta (encripta.org)

Quem Somos Nós

- O Encripta é um coletivo formado em junho de 2016 por alunas e alunos de graduação da Unicamp
- Lutamos pela segurança, proteção à privacidade, autonomia e liberdade das pessoas na internet
- É a nossa primeira oficina fora da Unicamp, então dá um desconto :)

Apresentação

- **Emails:** como usar *PGP* para troca de emails seguros, com os programas *Mailvelope* e *Thunderbird+Enigmail*
- **Criptrografia de Arquivos:** ensinaremos a criptografar arquivos e discos com a ferramenta *VeraCrypt*
- **Navegador:** como usar o *Tor Browser* para navegar de forma anônima e segura
- **Comunicação:** como usar o *Signal* e o *Jitsi* para conversar de forma segura

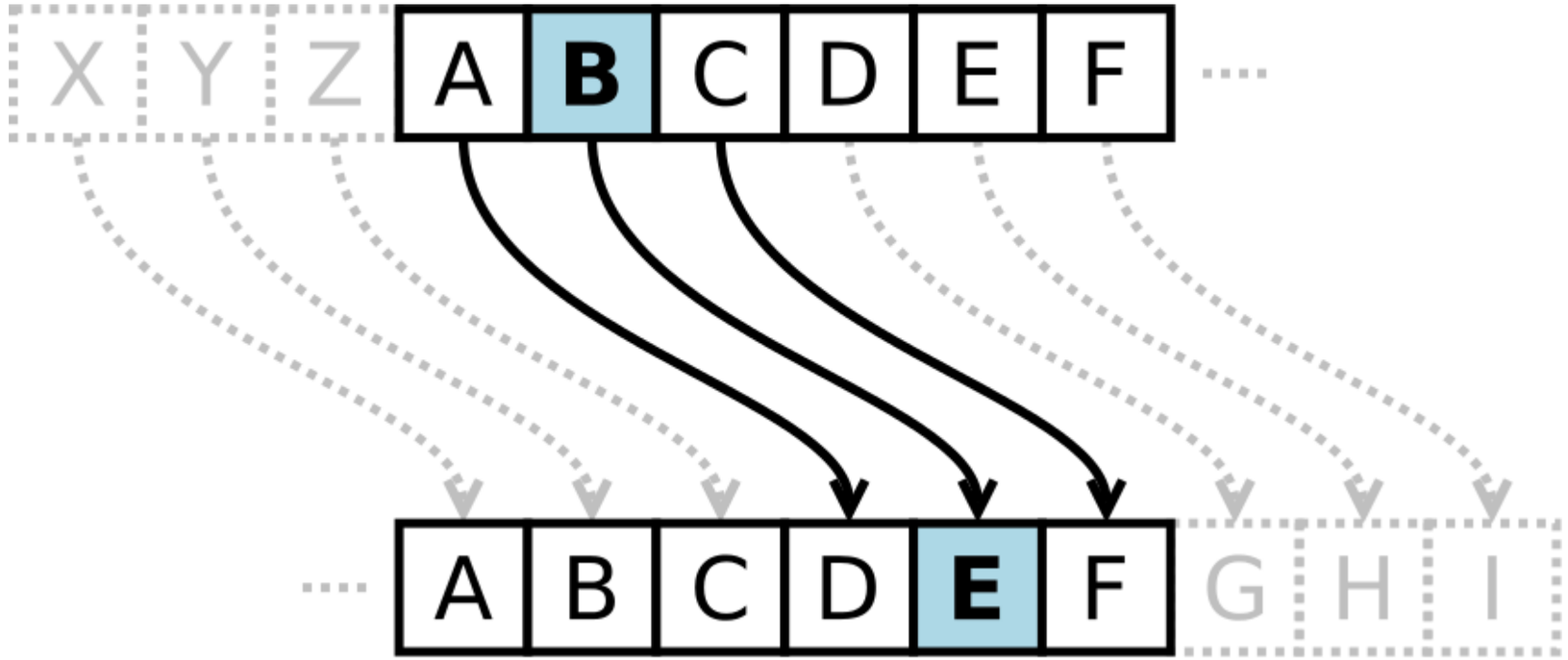
Criptografia

Conceitos básicos

História da Criptografia

Cifra de César

- Consiste numa *criptografia de substituição*, na qual cada letra do alfabeto será substituída por outra que está abaixo dela a um número **k** fixo de vezes. Denotaremos k como chave.



História da Criptografia

Cifra de César - Criptografando uma mensagem

- Para **k=3**, como na imagem, obtemos o seguinte alfabeto:
  * **normal:** ABCDEFGHIJKLMNOPQRSTUVWXYZ
  * **cifrado:** XYZABCDEFGHIJKLMNOPQRSTUVW
- Assim, para criptografar uma mensagem, basta escrevê-la de acordo com o alfabeto cifrado:
  * **normal:** CASA ARRANHADA
  * **cifrada:** ZXPX XOOXKEXAX

História da Criptografia

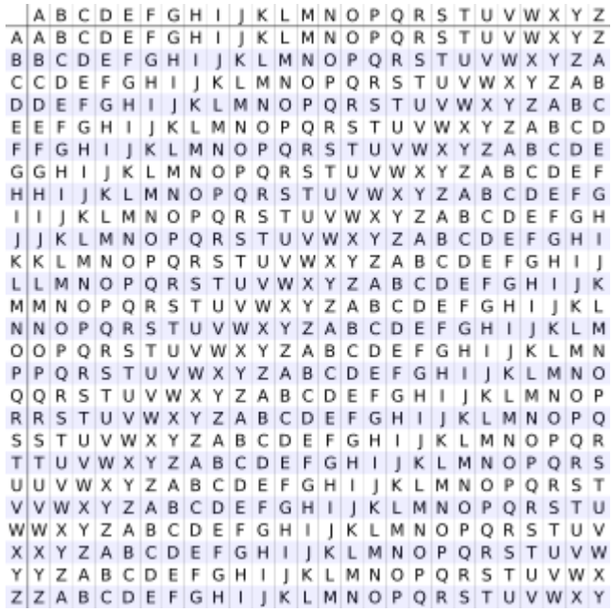
Cifra de César - Decifrando

- A cifra de César é facilmente decifrada mesmo quando se tem apenas o texto cifrado, pois conhecendo a língua na qual foi escrita a mensagem podemos analisar repetições e padrões comuns àquela língua
- Quando sabemos que este método foi utilizado, mas desconhecemos k (valor de troca), podemos testar as possíveis chaves num *ataque de força bruta*

História da Criptografia

Cifra de Vigenère

- Trata-se de uma *cifra polialfabética*, que se utiliza de uma série de cifras 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
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

História da Criptografia

Cifra de Vigenère - Método

Consiste na aplicação de uma série de cifras de César baseado em uma *palavra-chave*

- Escreve A-Z em termos de números inteiros 0-25 e defina uma palavra-chave
- Escreve a palavra-chave repetidas vezes até que essa obtenha o mesmo comprimento da mensagem a ser codificada:
  * mensagem: GOSTODEBATATA (13 caracteres)
  palavra-chave: FRITAFRITAFRI (13 caracteres)

História da Criptografia

Cifra de Vigenère - Método

- Cada letra da palavra-chave representa um **k** na Cifra de César.
  Na palavra-chave, temos que F é a sexta letra do alfabeto, então usaremos k=5 para codificar G da mensagem. Repete-se o processo até que tenha toda a mensagem codificada.

História da Criptografia

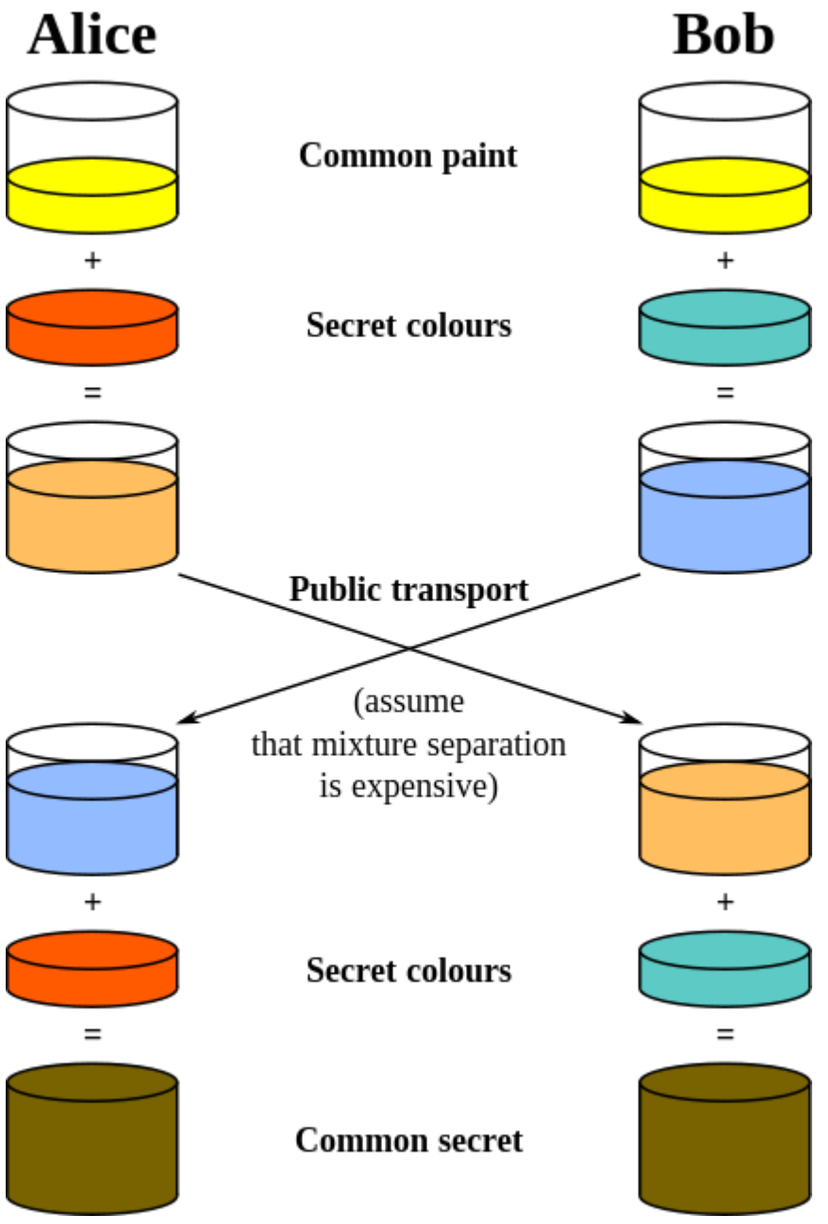
Diffie-Hellman

Para usar a criptografia simétrica, Alice e Bia precisam de alguma forma ter a mesma chave. Elas podem se encontrar pessoalmente e trocá-las, ou utilizar métodos como o Diffie-Hellman para trocar uma chave mesmo estando distantes.

História da Criptografia

Diffie-Hellman - Algoritmo:

- Alice e Bia combinam uma base **g** e um primo **p** (públicos).
- Alice e Bia criam, cada uma, números inteiros **a** e **b** (secretos).
- Alice calcula **g^a mod p** envia para Bia. Bia calcula **g^b mod p** e envia a Alice.
- Para concluir, Alice eleva o que recebeu a **a** e tira o resto **mod p**. Bia eleva o que recebeu a **b** e tira o resto **mod p**.
- As duas terminam tendo o valor **g^ab (mod p)**, e qualquer pessoa que interceptou as mensagens não tem acesso a esse valor. Esse valor pode ser usado como chave pública!


Alice
Bob
Common paint
+
Secret colours
=
Public transport
(assume
that mixture separation
is expensive)
+
Secret colours
=
Common secret

História da Criptografia

RSA:

- Uma das mais amplamente utilizadas no mundo
- Criptografia de chave pública
- A segurança é baseada na dificuldade de fatorar um inteiro em produto de primos

História da Criptografia

RSA - Método:

Vamos criar um par de chaves privada e pública no esquema RSA

- Escolha **p** e **q** primos (grandes). Defina **N=pq**
- Escolha algum **e** relativamente primo a **(p-1)(q-1)** (isto é, o mdc é 1)
- Encontre **d** tal que **ed = 1 mod (p-1)(q-1)**
- Definimos, então, a chave pública o par **(N,e)**, e a chave secreta **d**

História da Criptografia

RSA - Criptografar uma mensagem:

- A mensagem que Alice quer enviar é o número **M**
- Para encriptar **M** Alice faz **C = M^e mod N** com a chave pública **(N,e)** de Bia. **C** é o texto cifrado, que será transmitido para Bia, e que alguém que interceptar não vai entender
- Para decriptar **C**, Bia faz **C^d mod N** com sua chave secreta **d** e o resultado será a mensagem **M**

História da Criptografia

RSA - Segurança:

A segurança deste método é baseada na dificuldade de fatorar **N** no produto de primos **pq**. Se alguém souber os primos **p** e **q** deste produto, é muito fácil calcular **d** a partir da equação **ed = 1 mod (p-1)(q-1)** e quebrar a criptografia RSA!

Criptografia de Emails

Criptografia de Emails

Mailvelope

- Uma extensão para Firefox ou Chrome que permite criar e gerenciar chaves
- Não requer privilégios de administrador para ser instalado
- Para mais segurança, seu navegador deve estar sempre atualizado

Criptografia de Emails

Mailvelope

- Instale a extensão Mailvelope no site mailvelope.com
- Após instalar, o ícone do Mailvelope aparecerá na barra de extensões do navegador

Chave:

- Clique no ícone do Mailvelope, e depois em Opções. Haverá uma opção para importar chaves (caso você já tenha usado PGP alguma vez na vida) e uma opção para criar chaves

Criptografia de Emails

Mailvelope

Criando uma chave

- Clique em "Gerar chave"
- Insira *Nome*, *email*, e *senha*, que será usada para guardar seguramente a chave secreta
- Clique em "Gerar" e pronto! Você tem sua chave PGP

Para ver sua chave PGP recém gerada, basta entrar no menu "Exibição de Chaves" e clicar na sua chave. Neste menu, é possível ler dados da chave, exportar a chave públicar pra divulgar pras amigas, e exportar uma cópia da chave secreta pra guardar.

Criptografia de Emails

Mailvelope

Importando chaves públicas

Nas Opções no Mailvelope, há um item chamado Importar chaves. Aqui, é possível adicionar o arquivo da chave pública que alguém lhe enviou, ou pesquisar pelo nome/email de alguém num servidor público de chaves.

É necessário importar a chave de todos para quem você quer mandar emails.

Criptografia de Emails

Mailvelope

Enviando emails

Vamos supor que você quer enviar um email criptografado. Ao abrir seu webmail, e clicar em escrever, Mailvelope automaticamente adiciona um botão para criptografar mensagens: 

Clicando neste ícone, abre-se uma janela do Mailvelope onde é possível adicionar destinatários (que você importou) e um corpo da mensagem para criptogafar.
Dentro de "opções" é ainda possível assinar a mensagem para garantir autenticidade.

Criptografia de emails

Enigmail+Thunderbird

- **Thunderbird:** programa para gerenciar contas de email de forma prática e segura.
- **Enigmail:** uma extensão do Thunderbird que permite a criação e o gerenciamento de chaves públicas.

Criptografia de emails

Enigmail+Thunderbird

- Configure sua conta de email no Thunderbird
- **Adicionando o Enigmail:** em extensões, procure pelo Enigmail e clique em instalar. Após a instalação, reinicie o Thunderbird
- Aparecerá um assistente de configuração.
  - Caso não apareça, vá em Enigmail > Assistente de Configuração (Setup Wizard)
- Escolha o email para o qual deseja criar o par de chaves
- Crie uma **senha forte** para proteger sua chave

Criptografia de emails

Enigmail+Thunderbird

- Crie um **certificado de revogação** e o salve num pendrive, CD ou mídia, que esteja guardada em local seguro.
    - caso perca sua chave ou ela for comprometida, somente poderá desativá-la com esse certificado
- **Achando as chaves públicas:** no Enigmail, vá em Gerenciamento de Chaves> Keyserver > Procurar por Chaves e digite o email, nome ou ID da chave da pessoa

Criptografia de emails

Enigmail+Thunderbird

- **Enviando email criptografado:** importe a chave pública da pessoa > vá em escrever nova mensagem > clique no cadeado e digite a senha da sua chave privada
- 0 ssd.eff.org oferece um tutorial completo de como usar o Enigmail

Criptrografia de Arquivos e Disco

Criptografia de Arquivos e Disco

VeraCrypt

- Surgiu como uma ramificação (fork) do TrueCrypt, após o mesmo ser descontinuado
  - veracrypt.codeplex.com/releases/view/629329
- Com o VeraCrypt você pode
  - criar containers criptografados;
  - criar volumes ocultos (hidden volumes);
  - criptografar pendrives, cartões de memórias e HDs inteiros.

Criptografia de Arquivos e Disco

VeraCrypt - Containers criptografados

- Criação de um "cofre" criptografado no seu HD para salvar os arquivos de forma segura
- Possibilidade de escolher o algoritmo de criptografia e de hash que serão usados
- Cenários em que pode ser útil:
  - armazenar arquivos pessoais no computador do trabalho;
  - armazenar arquivos em pendrives que usa para impressões.

Criptografia de Arquivos e Disco

VeraCrypt - Containers criptografados

- **Criando o volume:** Create Volume > Create an encrypted file container > Standard VeraCrypt volume > escolha a localização do container > AES e SHA-512 > tamanho do container > senha > formato (selecione EXT4 se for usar apenas GNULinux, caso contrário, vá de FAT) > mexa loucamente o mouse > pronto, seu volume está criado
- **Montando o volume:** na parte volume, selecione o arquivo do volume > select file > coloque a senha > mount
- **Desmontando o volume:** na parte volume, clique em dismount

Criptografia de Arquivos e Disco

VeraCrypt - Volumes ocultos

- Criação de um container externo criptografado com um volume oculto
- Não é possível saber que existe um volume oculto, apenas que há o container externo criptografado
- **Ideal:** colocar coisas não-sensíveis no container externo criptografado e as coisas realmente sensíveis no oculto

Criptografia de Arquivos e Disco

VeraCrypt - Volumes ocultos

- **Criação da camada externa do container:** Create Volume > Create an encrypted file container > Hidden VeraCrypt volume > escolha a localização do container > AES e SHA-512 > tamanho do container (tamanho total, com a parte oculta) > senha da parte externa > mexa o mouse loucamente
- Após esse processo, clique em "Open Outer Volume" e salve alguns arquivos na partição externa. Feito isso, clique em next.

Criptografia de Arquivos e Disco

VeraCrypt - Volumes ocultos

- **Criação da partição oculta:** AES e SHA-512 > escolha o tamanho do container oculto (menor que o container total) > senha da parte oculta (deve ser **diferente da senha da parte externa**) > formato da partição > mexa o mouse loucamente > pronto

Criptografia de Arquivos e Disco

VeraCrypt - Volumes ocultos

- Há duas **senhas diferentes**, uma pro volume oculto e uma pro volume externo,
  - para abrir o **volume oculto** basta fazer a mesma coisa do container criptografado e colocar a senha do volume oculto;
  - para abrir o **volume externo**, coloque a senha do volume externo.
- Caso as senhas sejam iguais só conseguirá abrir o container externo (faça o teste!)

Criptografia de Arquivos e Disco

VeraCrypt - Criptografia de disco total e pendrives

- Criptografa toda a partição, não apenas um container
- **Utilidade:**
  - criar backups criptografados;
  - carregar pendrives com informações sensíveis.

Criptografia de Arquivos e Disco

VeraCrypt - Criptografia de disco total e pendrives

- Create Volume > escolha entre Normal ou Oculto > selecione a partição ou pendrive que deseja criptografar (isso **apagará todos os dados** da partição selecionada)

Navegação Anônima e Segura

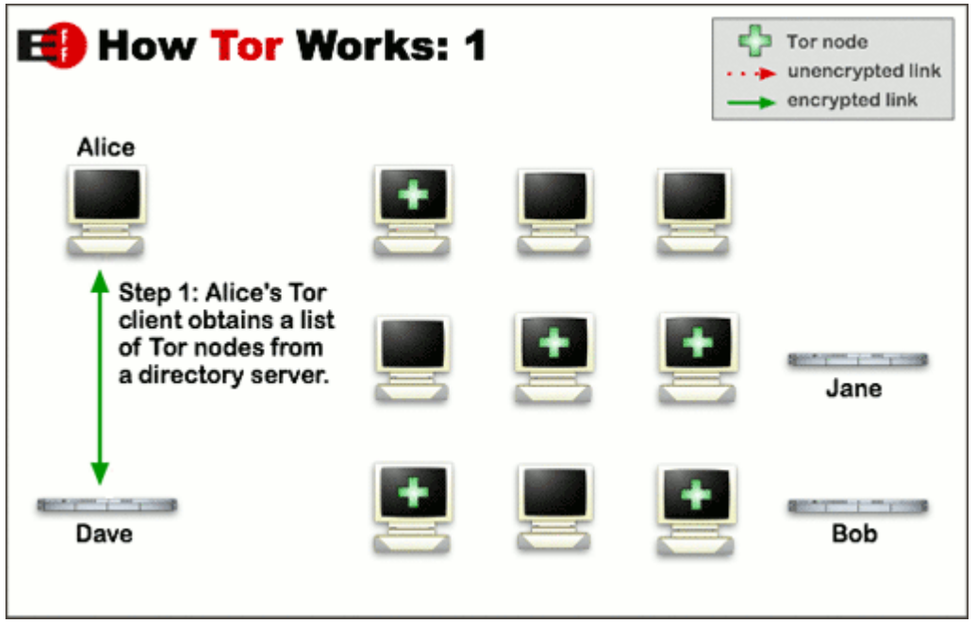
Navegação Anônima e Segura

Tor Browser

- Um navegador de internet seguro e anônimo. O Tor criptografa todos os dados, além de passá-los por 3 servidores antes de chegar a você, dificultando o rastreamento dos dados e garantindo anonimato
- Para usar o Tor Brwoser, basta baixar o programa em torproject.org, descompactar a pasta e executar o arquivo. Não é necessário instalar
- Recomendações: ativar o bloqueamento de scripts ao abrir o navegador (no canto superior esquerdo), e averiguar as configurações do Tor no ícone da cebola, também no canto superior esquerdo

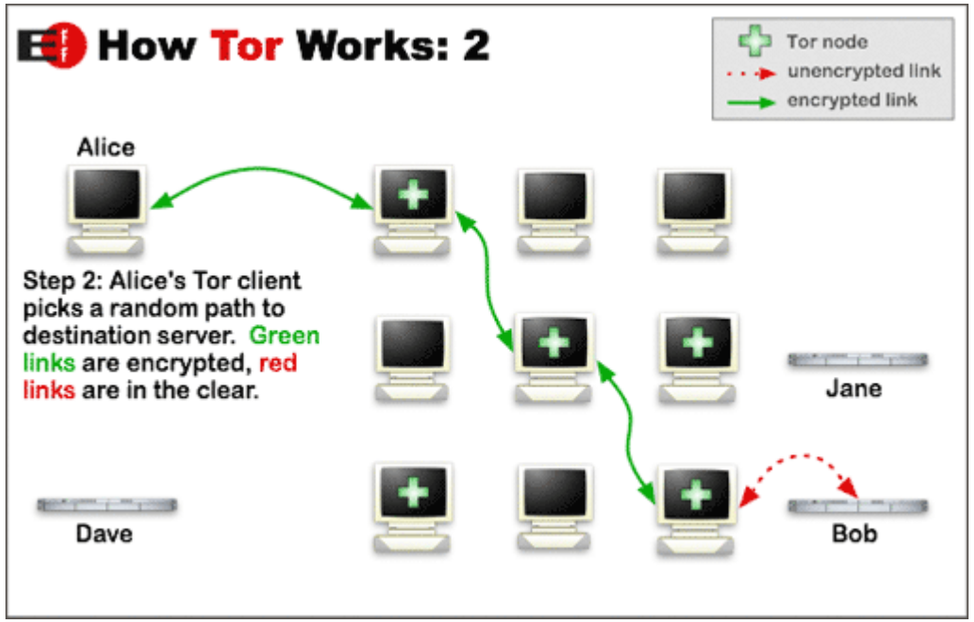
Navegação Anônima e Segura

Tor Browser - Como Tor funciona



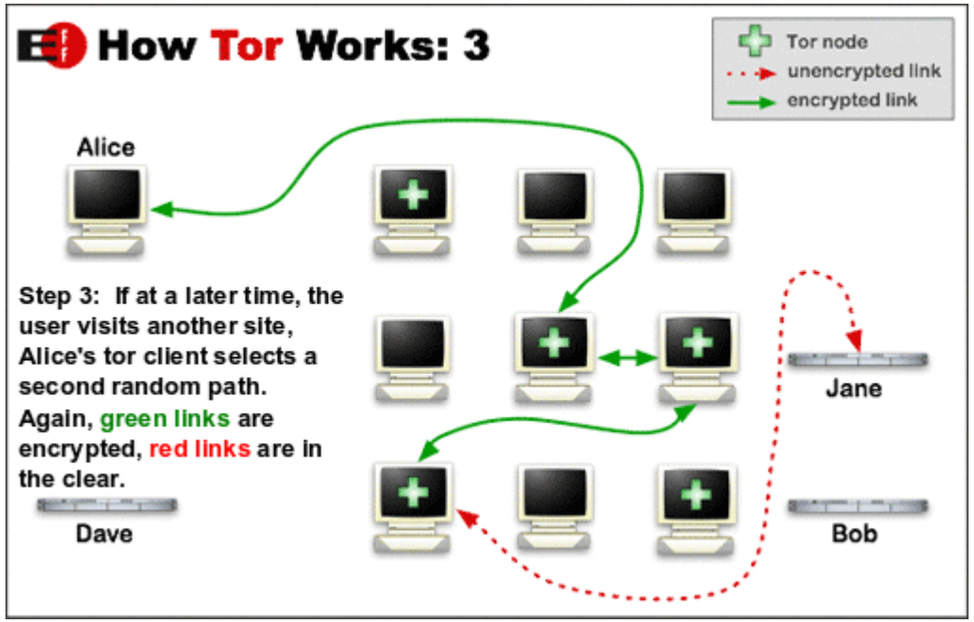
Navegação Anônima e Segura

Tor Browser - Como Tor funciona



Navegação Anônima e Segura

Tor Browser - Como Tor funciona



Navegação Anônima e Segura

Navegadores

Cookies

Uma das formas como as empresas podem rastrear usuários na internet é através de *cookies*. Cookies são dados que são salvos em seu navegador, e que podem ser acessados pelos sites. É a forma como sites deixam os usuários logados mesmo depois de fechar o navegador.

Navegação Anônima e Segura

Navegadores

Cookies

Porém muitas empresas e serviços usam cookies para salvar os sites que usuários acessam, e como eles se comportam, para construir um perfil dos mesmos. Formas de se proteger contra isso são:

- Bloqueando cookies de terceiros, faz com que serviços de propaganda não possam salvar cookies
- Marcar para deletar cookies ao sair do navegador

Comunicação Segura

Comunicação Segura

Signal

- Aplicativo software livre disponível para Android e iOS
- Permite mensagens de texto, áudio, imagens e chamadas de áudio
- WhatsApp usa o protocolo do Signal, que possui criptografia de ponta-a-ponta

Comunicação Segura

Jitsi

- Serviço para conferências de áudio e vídeo (tipo Skype, Hangouts, etc)
- Não é necessária instalação, roda direto no navegador: meet.jit.si
- Para convidar alguém para a chamada só precisa passar o link da chamada. ex: meet.jit.si/conversamaneira
- Tem funções interessantes, como levantar a mão para falar, chat e compartilhar tela

Cifra-te ou te devoram

Cifra-te ou te devoram

S&nh5s

- As senhas precisam ser **fáceis de memorizar** e **difíceis para um computador adivinhar**;
- Em 2013, Edward Snowden disse:
  Presuma que seu adversário é capaz de realizar um trilhão de tentativas por segundo.

Cifra-te ou te devoram

S&nh5s - boas práticas

- **Não use a mesma senha em serviços diferentes**, ex: email, site de compras, facebook;
- **Mude as senhas periodicamente:** pode ser a cada 3 ou 6 meses. O KeepassX tem a opção de expirar as senhas após um certo tempo;
- **Não coloque informações pessoais nas suas senhas**, ex: data de nascimento sua ou de pessoas próximas, nomes de familiares, animal de estimação, etc;
- Use um gerenciador de senhas e mantenha uma cópia deste num local seguro fora do computador (exemplo: hd externo);
- Para senhas que não podem ser armazenadas no gerenciador, use um método como o *Dadoware*.

Cifra-te ou te devoram

S&nh5s - Dadoware

- É um método de criação de senhas fortes e aleatórias;
- Requer pelo menos um dado (ou gerador de números aleatórios) e o livreto de palavras: github.com/thoughtworks/dadoware/blob/master/livreto/dadoware-lista.pdf
- Um guia para uso está disponível em: github.com/thoughtworks/dadoware/blob/master/livreto/dadoware-intro.pdf

Cifra-te ou te devoram

S&nh5s - Dadoware (exemplo)

- Jogue 5 dados 6 vezes (ou um dado 30 vezes) e anote os resultados;
- Cada uma das 5 jogadas corresponde a uma palavra da sua senha.
    - Recomenda-se que use seis palavras. Mas sinta-se livre para fazer com números maiores.

Cifra-te ou te devoram

S&nh5s - Dadoware (exemplo)

- Os 2 primeiros valores representam a página da palavra e os outros 3 a localização da palavra na página;
- Por exemplo, a sequência 25342 corresponde à palavra "dentuça":
  - Página 2,5
  - Palavra 342
- Após repetir o processo, você terá 6 palavras aleatórias.

Cifra-te ou te devoram

- **Dicas para memorizar:**
  - forme uma frase com as palavras aleatórias;
  - anote as palavras num papel até decorar (depois disso jogue fora o papel).
- Embora não faça análise de engenharia social, para verificar o quão seguro a senha é temos:
  - howsecureismypassword.net

Cifra-te ou te devoram

S&nh5s - Gerenciadores de Senhas

- Permite criar, organizar e armazenar senhas;
- Os gerenciadores geram um arquivo que contém todas suas senhas. Esse arquivo é protegido por uma senha, que deve ser bem forte (Dadoware);
- Permite usar senhas fortes e diferentes para cada serviço, sem a necessidade de memorizar cada uma delas;

Cifra-te ou te devoram

S&nh5s - Gerenciadores de Senhas

- **Android:** KeepassDroid;
- **iOS:** iKeepass;
- **GNU/Linux, Windows ou Mac OS:** KeepassX
  - www.keepassx.org/downloads

Cifra-te ou te devoram

S&nh5s - Gerenciadores de Senhas

Dica pro KeepassX:

Vá em Banco de Dados > Configuração do Banco de Dados > Rodadas de Transformação e clique no reloginho para aumentar a quantidade de "contas" que o computador terá que fazer para desbloquear seu arquivo de senhas.

- Isso faz com que um atacante tenha maior dificuldade em descobrir sua senha pelo método de tentativa e erro, pois cada tentativa leva vários segundos.

Cifra-te ou te devoram

Criptografia como ferramenta política

Ao trabalhar em agências governamentais, grandes empresas ou redes midiáticas, as pessoas podem se deparar com informações sensíveis -- como, por exemplo, desvios de dinheiro, ligação com tráfico ou ações que firam os direitos e liberdades de demais pessoas.

Quando isso ocorre, podem agir de duas formas: ficar caladas e ser coniventes ou tomar atitude frente aos abusos. Caso optem pela segunda opção, precisam de ferramentas que assegurem o anonimato, a fim de vazarem informações sem colocar em risco suas liberdades.

Cifra-te ou te devoram

Criptografia como ferramenta política - exemplos famosos

- **Chelsea Manning**, ex-militar dos EUA, coletou e divulgou milhares de arquivos sigilosos do exército de seu país. Um desses arquivos é o famoso vídeo do ataque aéreo em Bagdá mostrando os chamados "danos colaterais".
- **Edward Snowden**, ex-administrador de sistemas da CIA e ex-contratado da NSA, tornou públicos os detalhes de vários programas que constituem o sistema de vigilância global da NSA.

Cifra-te ou te devoram

Criptografia como ferramenta política - Vazando informações

Caso se depare com informações sigilosas de interesse público, provavelmente não poderá divulgá-las sem sofrer consequências legais. Porém, felizmente, hoje em dia temos ferramentas que possibilitam **vazar dados de modo anônimo e seguro**.

Cifra-te ou te devoram

Criptografia como ferramenta política - Vazando informações

As sugestões contidas aqui são SUGESTÕES e podem não ser válidas para todas situações. **Não arrisque sua liberdade apenas seguindo esses slides!**

- **Silêncio, uma regra de ouro:** quanto menos gente souber que você é um informante, melhor, tanto pra você como pras outras pessoas;

Cifra-te ou te devoram

Ciptografia como feramente política - Vazando informações

- **Volume Oculto:** essa ferramenta pode ser usada para copiar arquivos sigilosos, que serão entregues a alguém que irá publicá-los ou levados para um local seguro para enviá-los posteriomente com o *SecureDrop*;
- **Tor:** é essencial para manter o anonimato ao mandar os arquivos ou conversar com entidades que publicarão os arquivos. **Apenas pesquise sobre vazamentos usando o Tor, usar um navegador comum pode te entregar.**

Cifra-te ou te devoram

Criptografia como ferramenta política - Vazando informações

- **SecureDrop:** sistema para envio de arquivos de maneira anônima, criado justamente para pessoas vazarem informações sigilosas e permanecerem seguras. **Só é possível enviar informações com o SecureDrop usando a rede Tor**.

Cifra-te ou te devoram

Criptografia como ferramente política - Vazando informações

Caso for vazar informações, **só acesse os links a seguir usando o Tor ou outra conexão anônima**:

- guia de como enviar informações para o The Intercept (em português): theintercept.com/2016/08/02/como-enviar-informacoes-para-the-intercept
- manual do SecureDrop sobre como liberar informações (em inglês): docs.securedrop.org/en/stable/source.html
- diferentes jornais, agências e organizações que usam o SecureDrop: securedrop.org/directory

Cifra-te ou te devoram

Criptografia

Ainda que use criptografia em emails, arquivos, navegador e comunicação, **você não estará 100% seguro**, então siga sempre as boas práticas de segurança!

Cifra-te ou te devoram

Criptografia - Boas práticas de segurança

- Mantenha sempre seus programas e sistema operacional atualizados
- Habilite a autentificação em duas etapas
- Utilize senhas fortes e não repetidas, além de lembrar de trocá-las com frequência
    - o KeepassX permite definir uma data de expiração para cada senha

Cifra-te ou te devoram

Criptografia - Boas práticas de segurança

- Faça backups
- Cuidado com o que abre no navegador, com os anexos e links estranhos
- Cuidado com o que instala

Cifra-te ou te devoram

Criptografia e Privacidade:

- Por mais clichê que pareça, **com grande poderes, vem grandes responsabilidades**
- **Respeite a privacidade das pessoas**.