Direitos humanos e tecnologias da vigilância

Por que a criptografia é essencial aos direitos humanos

Rodolfo Avelino
UFABC - 2018

Desvende...

gluhlwrv kxpdqrv

Segredo....

Direitos Humanos

Notícias produzidas pela Artigo 19 >

Artigo 19 na mídia >

SALA DE IMPRENSA

01/06/2015 | Notícias

Criptografia e anonimato são essenciais para liberdade de expressão

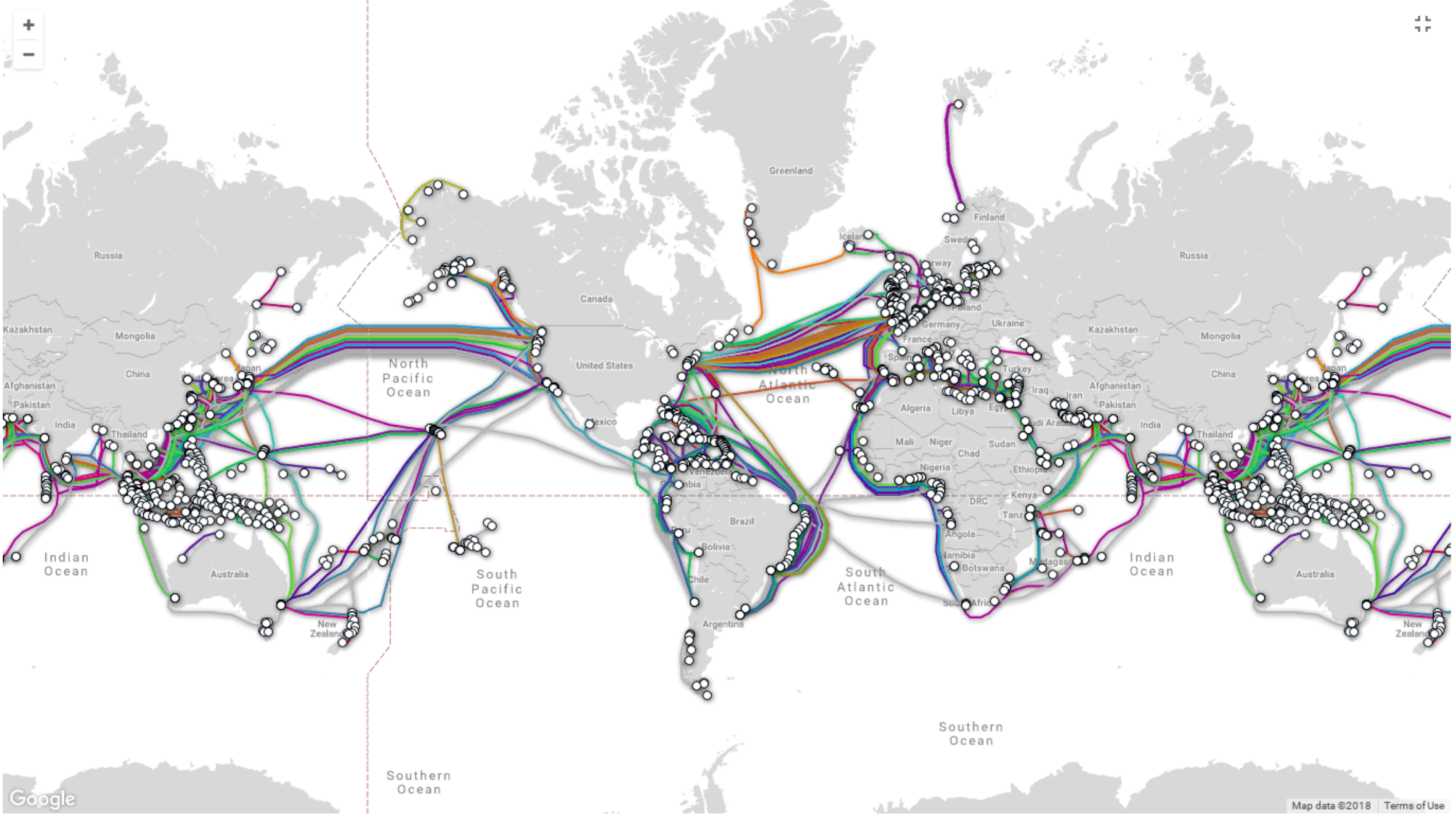
No último dia 28, o relator especial da ONU para Liberdade de Expressão, David Kaye, publicou seu **primeiro relatório anual** em que analisa a relação entre o direito de expressão e de opinião e direito à privacidade com o uso de criptografia e do anonimato na era digital. O documento avalia ainda os cenários em que governos podem impor restrições a essas práticas.

Criptografia

ferramenta essencial e necessária para proteger o direito à liberdade de opinião e expressão na era digital, conclui o relatório da Organização das Nações Unidas (ONU)

A criptografia, assim como o anonimato, é essencial para artistas, jornalistas, denunciantes e várias outras categorias

ONU


Greenland
Russia
Canada
United States
Mexico
Kazakhstan
Mongolia
China
Japan
Afghanistan
Pakistan
India
Thailand
Indonesia
Australia
New Zealand
Finland
Sweden
Norway
Iceland
Germany
France
Spain
Ukraine
Turkey
Iraq
Iran
Algeria
Libya
Egypt
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
DRC
Angola
Namibia
Botswana
Madagascar
South Africa
Brazil
Bolivia
Chile
Argentina
Venezuela
Colombia
Peru
North Pacific Ocean
South Pacific Ocean
North Atlantic Ocean
South Atlantic Ocean
Indian Ocean
Indian Ocean
Southern Ocean
Southern Ocean
Google
Map data ©2018
Terms of Use

Que consequências sociais, culturais e econômicas teremos com a captura de todo tipo de dado por parte das corporações?

Sérgio Amadeu

Troca da privacidade pelas experiências que as empresas podem proporcionar.

Sérgio Amadeu

Quem NÃO DEVE não TEME.

Programa de espionagem massiva

“Vivemos em um mundo no qual a vigilância em massa, ataques digitais aos indivíduos e à sociedade civil, o assédio de membros de grupos vulneráveis, e uma grande variedade de opinião e expressão digitais resultam em graves repercussões, incluindo detenções, agressões físicas e mesmo assassinatos”

David Kaye


The right to freedom of expression
Guaranteed under Article 19 of the ICCPR, it protects the right of people to send, seek and receive ideas and information.


The right to privacy
Under Article 17 of the ICCPR, it guarantees protection from "arbitrary or unlawful interference" with citizens' privacy, family, home and correspondence.

Liberdade de expressão

David Kaye, observou que a criptografia e o anonimato nas comunicações digitais merecem uma forte proteção para salvaguardar o direito dos indivíduos de exercer sua liberdade de opinião e expressão.

Privacidade

Privacidade

“O fim da privacidade nada mais seria que a indiferenciação entre o espaço privado e espaço público”

Sérgio Amadeu

A criptografia, ao fazer da comunicação incompreensível a não ser àqueles a que se destina, cria “uma zona de privacidade para proteger opiniões e crenças”

David Kaye

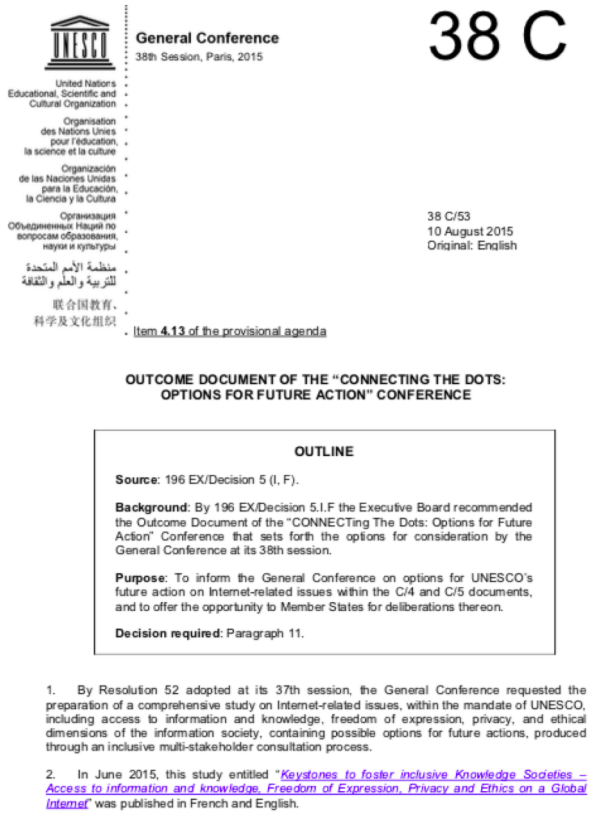
A Conferência “CONECTANDO OS PONTOS: OPÇÕES PARA A AÇÃO DO FUTURO”

Promovida pela UNESCO em março de 2015, foi observado o potencial da Internet para avançar o progresso humano em direção às Sociedades do Conhecimento inclusivas.

A Conferência “CONECTANDO OS PONTOS: OPÇÕES PARA A AÇÃO DO FUTURO”

Reconheceram o seu importante papel e afirmaram os princípios de direitos humanos que sustentam a abordagem da UNESCO às questões relacionadas à Internet, especificamente que os mesmos direitos que as pessoas têm off-line devem ser protegidos on-line, conforme a resolução A/HRC/RES/26/13 do Conselho de Direitos Humanos

CONNECTing the Dots Outcome Document



United Nations Educational, Scientific and Cultural Organization
Organisation des Nations Unies pour l'éducation, la science et la culture
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
Организация Объединенных Наций по вопросам образования, науки и культуры
منظمة الأمم المتحدة للتربية والعلم والثقافة
联合国教育、科学及文化组织

General Conference
38th Session, Paris, 2015

38 C

38 C/53
10 August 2015
Original: English

Item 4.13 of the provisional agenda

OUTCOME DOCUMENT OF THE "CONNECTING THE DOTS: OPTIONS FOR FUTURE ACTION" CONFERENCE

OUTLINE

Source: 196 EX/Decision 5 (I, F).

Background: By 196 EX/Decision 5.I.F the Executive Board recommended the Outcome Document of the "CONNECTing The Dots: Options for Future Action" Conference that sets forth the options for consideration by the General Conference at its 38th session.

Purpose: To inform the General Conference on options for UNESCO's future action on Internet-related issues within the C/4 and C/5 documents, and to offer the opportunity to Member States for deliberations thereon.

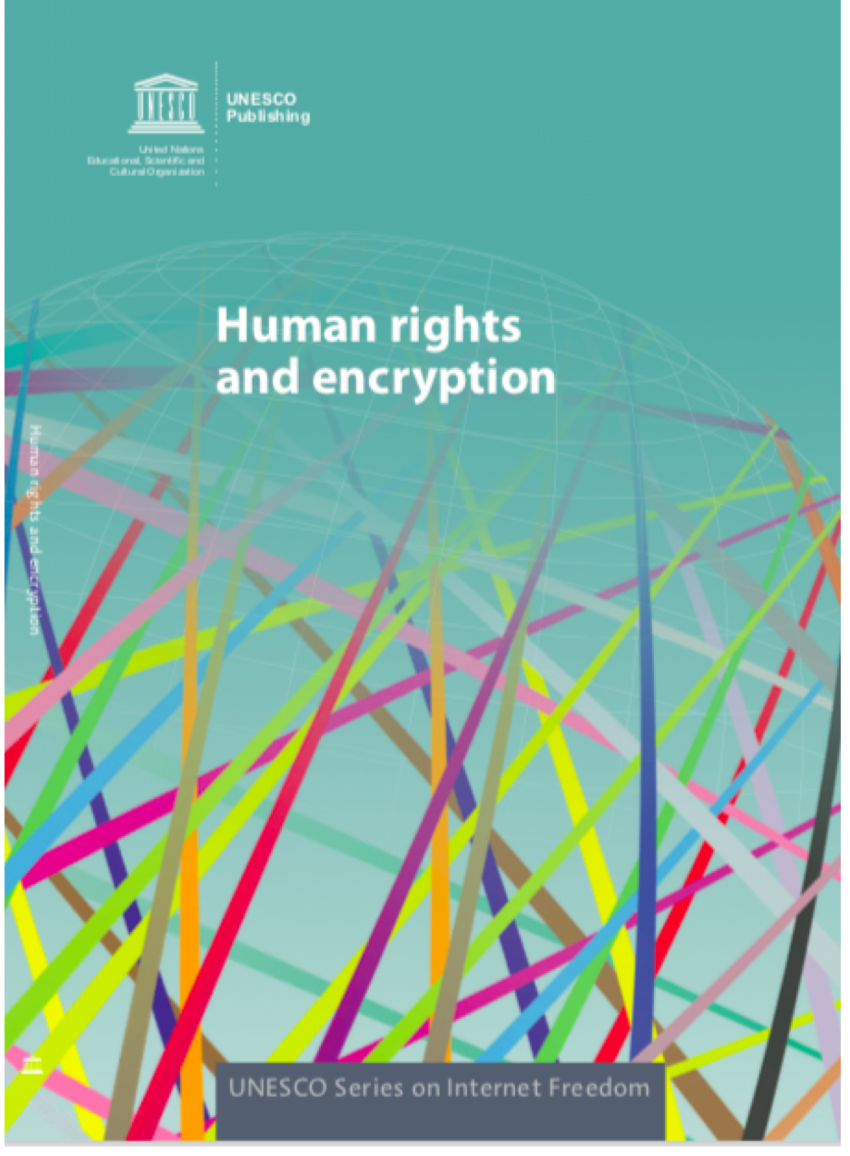
Decision required: Paragraph 11.

1. By Resolution 52 adopted at its 37th session, the General Conference requested the preparation of a comprehensive study on Internet-related issues, within the mandate of UNESCO, including access to information and knowledge, freedom of expression, privacy, and ethical dimensions of the information society, containing possible options for future actions, produced through an inclusive multi-stakeholder consultation process.

2. In June 2015, this study entitled "*Keystones to foster inclusive Knowledge Societies – Access to information and knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet*" was published in French and English.

Options for UNESCO related to Privacy

Reconhecer o papel que o anonimato e a criptografia podem desempenhar como facilitadores da proteção da privacidade e da liberdade de expressão e facilitar o diálogo sobre essas questões.


UNESCO
Publishing
United Nations
Educational, Scientific and
Cultural Organization
Human rights and encryption
Human rights and encryption
UNESCO Series on Internet Freedom


Criptografia

A Criptografia consiste na ciência (e arte) da transformação de texto simples em texto ilegível, de tal modo que apenas quem saiba qual o processo de reverter a transformação possa recuperar o texto original.

Na sociedade informacional

Criptografia

Criptografia etimologia (Houaiss)

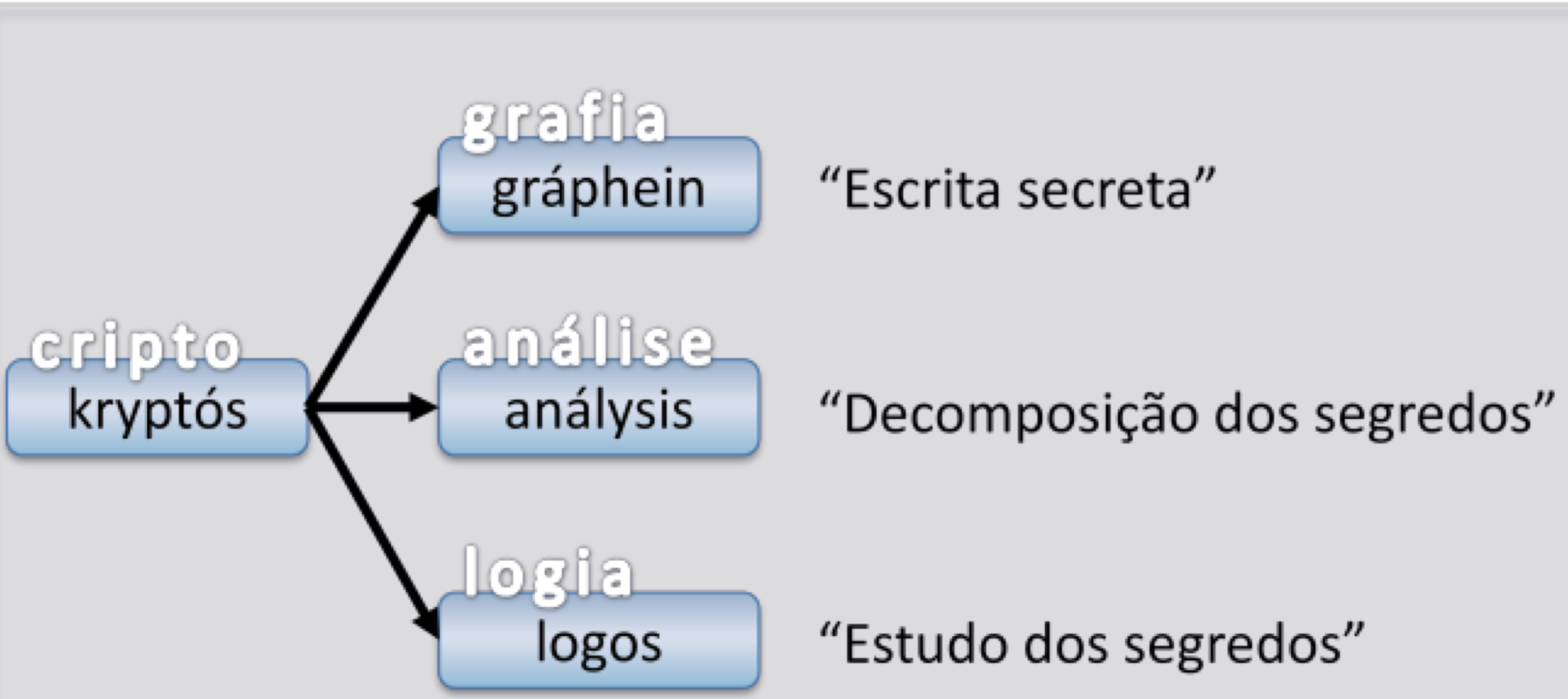
cript(o)- (gr. kruptós 'oculto, secreto, obscuro, ininteligível')

grafia (gr. -graphía, com o sentido de 'escrita', do v. gr. gráphō 'escrever')

Criptografia = ocultar a escrita

Criptologia = Estudo da criptografia

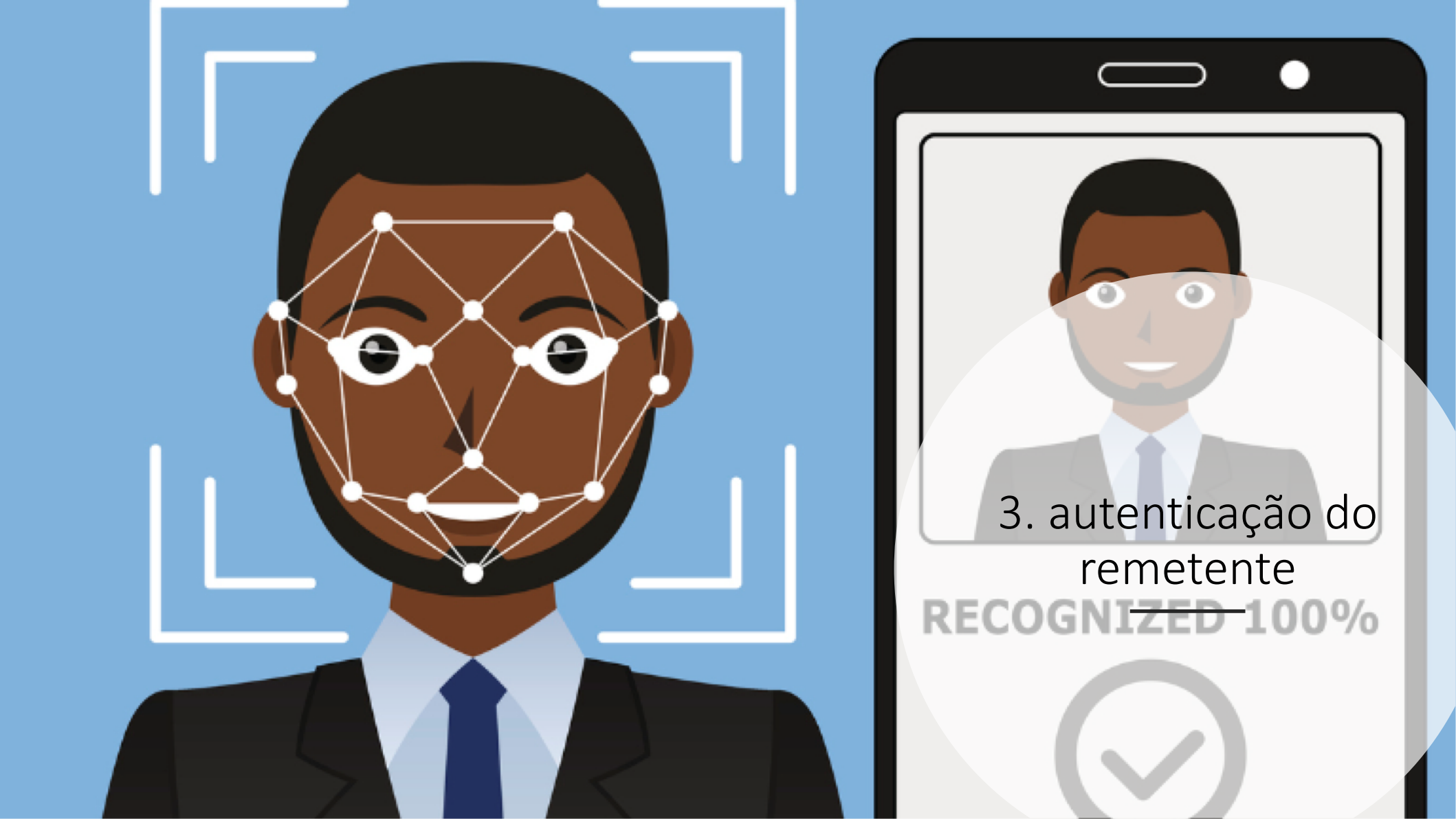
Criptoanálise = Quebra de criptografia


grafia
gráphein
"Escrita secreta"
cripto
kryptós
análise
análysis
"Decomposição dos segredos"
logia
logos
"Estudo dos segredos"

Criptografia

1. confidencialidade

2. Integridade de dados


3. autenticação do remetente
RECOGNIZED 100%

4 – Não repúdio ou irretratabilidade do remetente

Cifragem

Processo de converter uma informação comum (texto claro ou aberto) em algo não-inteligível

Decifragem

É a tarefa contrária, dado uma informação não-inteligível convertê-la em texto claro ou aberto.

Introdução

Encriptação é o processo de cifrar ou esconder a informação.

Decriptação é o processo de converter dados encriptados de volta a sua forma original.

Cifrar e Decifrar

Criptografia na computação

Exemplos:

- Sistemas de arquivos (HD, Pendrive);
- Mensagens eletrônicas (email);
- Conexão web segura (https);
- Mensagens instantâneas (Google talk e Messenger).

Introdução

Criptografia Clássica

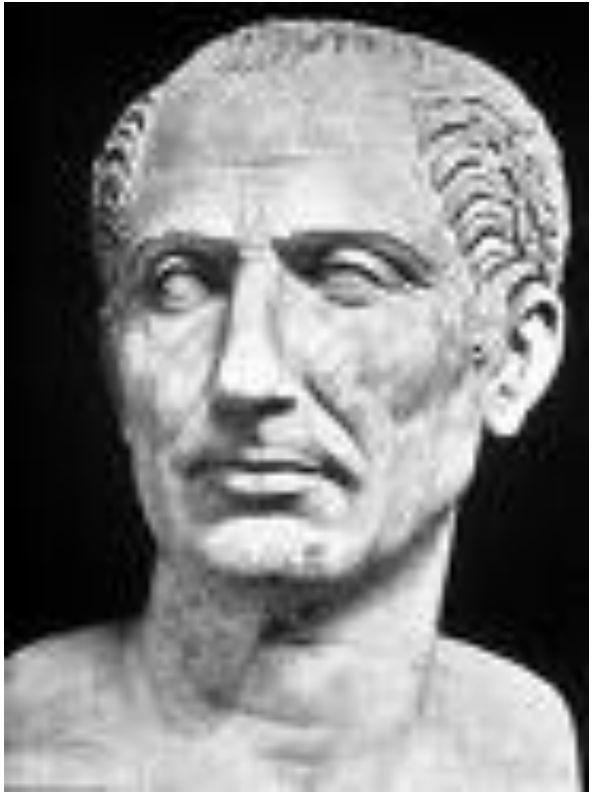
Ainda pouco influenciada pela Informática;
Algoritmos por Substituição e transposição;
Chave compartilhada (simétrico).

Criptografia Moderna

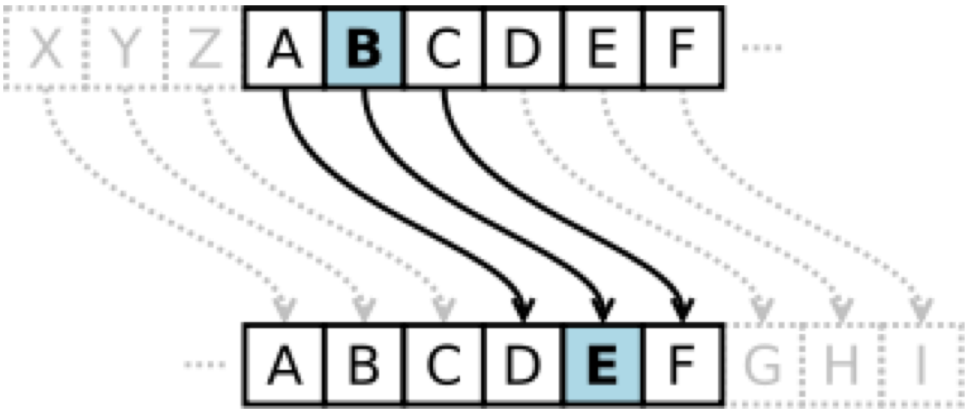
Maior influência da informática; Algoritmos assimétricos; Infraestrutura de chaves públicas.

Clássica - Cifra de Cesar

Também conhecida como cifra de troca, código de César ou troca de César, é uma das mais simples e conhecidas técnicas de criptografia. O nome do método é em homenagem a Júlio César, que o usou para se comunicar com os seus generais.



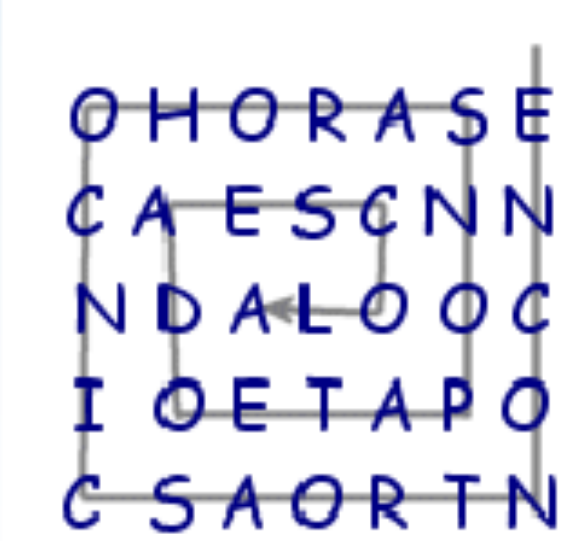
Cifra de César



A ação de uma cifra de César é mover cada letra do alfabeto um número de vezes fixo abaixo no alfabeto. Este exemplo está com uma troca de três, então o B no texto normal se torna E no texto cifrado.

Algoritmo Transposição

Cifras de transposição são imunes a análise de frequência, uma vez que as letras que estão no texto cifrado são as mesmas do texto em claro.



Algoritmos X Chaves

Todos os algoritmos devem ser públicos;

apenas as chaves são secretas.

Criptografia: Princípio

O resultado da criptografia depende de um parâmetro de entrada, denominado chave.

Chaves Criptográficas

- Os Algoritmos Modernos utilizam chaves binárias
- O espaço de chaves depende do tamanho da chave
- Chaves criptográficas são medidas em bits: 128 bits, 256 bits, 512 bits.....
- Uma chave de 56 bits tem um intervalo de 0 ate 2^{56} chaves (1 quatrilhão de chaves).

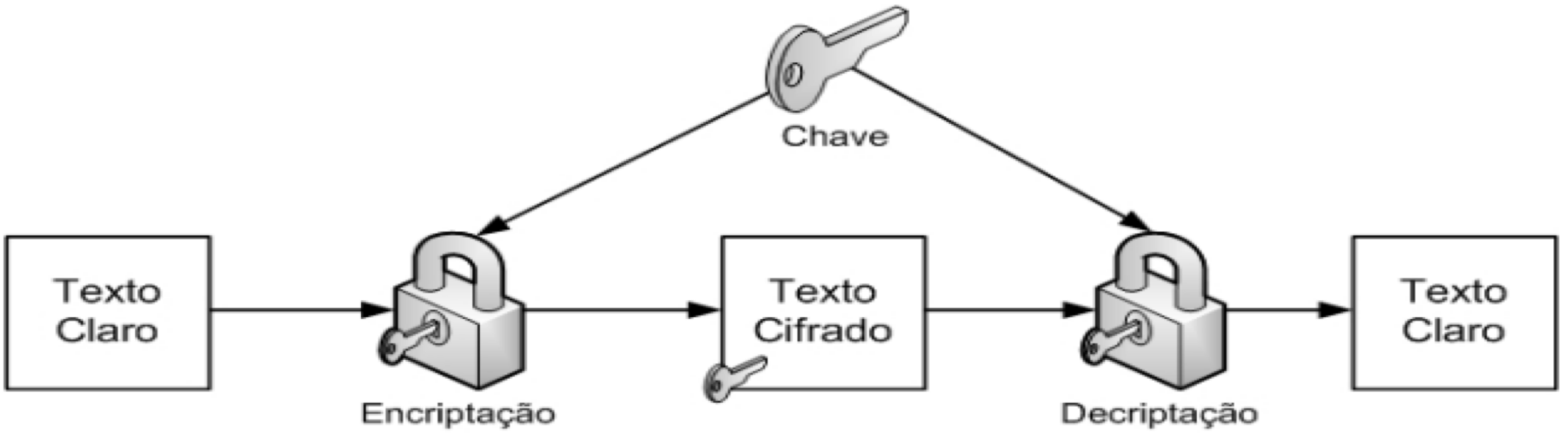
Existem dois tipos de Algoritmos

Simétrico

Assimétrico

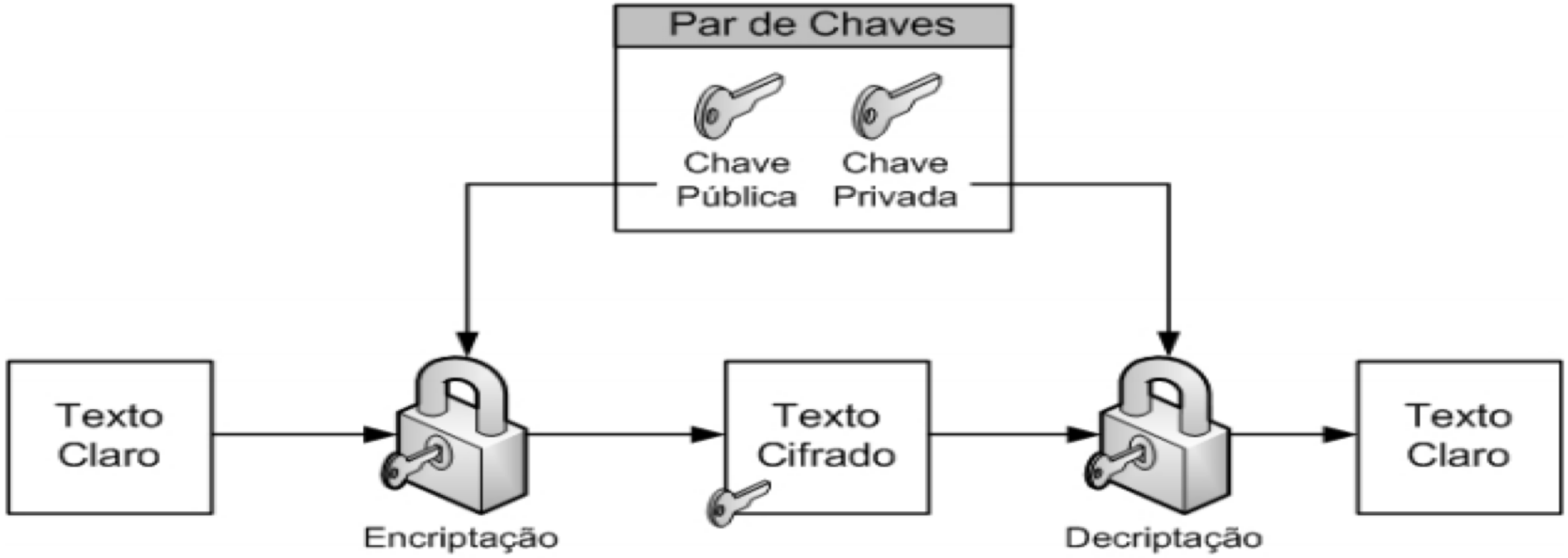
Criptografia Simétrica

A mesma chave é utilizada para cifrar e decifrar a mensagem (chave compartilhada)



Criptografia Assimétrica

Conhecida como infraestrutura de chaves públicas;
Possui um par de chaves : Chave Pública e Chave Privada

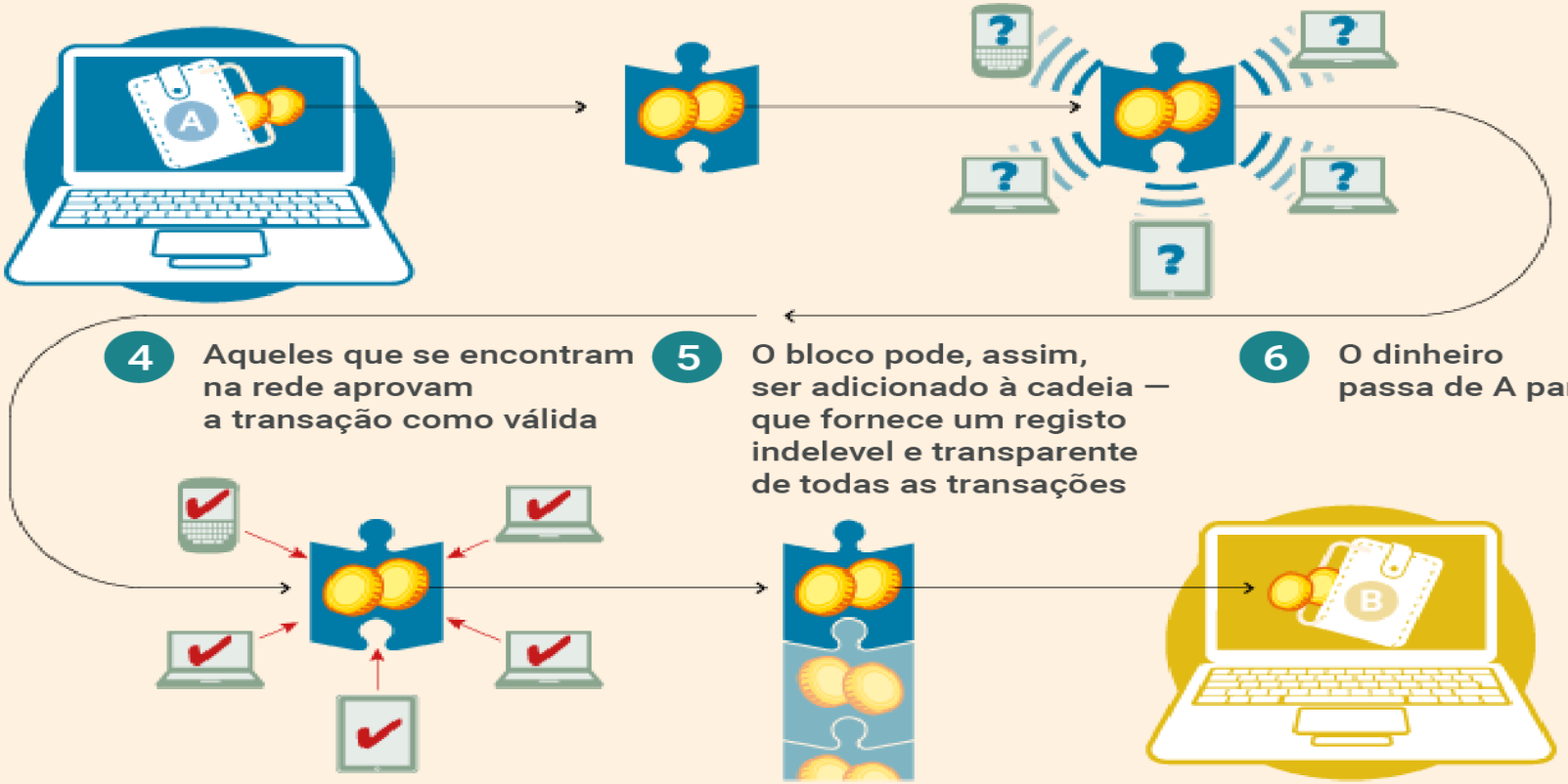


Criptografia Além da comunicação

BlockChain

Como funciona uma blockchain (cadeia de blocos)?

1. A quer enviar dinheiro a B
2. A transação é representada online como um "bloco"
3. O bloco é transmitido a todas as partes da rede
4. Aqueles que se encontram na rede aprovam a transação como válida
5. O bloco pode, assim, ser adicionado à cadeia — que fornece um registo indelevel e transparente de todas as transações
6. O dinheiro passa de A para B



Fonte: FT

Introdução

- Um banco de dados autônomo, progressivo, que mantém uma lista de registros ou transações.
- Cada bloco contém uma lista de registros, e cada bloco é encadeado com o anterior.
- Literalmente uma cadeia de blocos.

Distribuído

Não há uma entidade central que aprova as transações e estabelece normas.

Dois principais conceitos

Uma **rede de negócios segura**, na qual os participantes transferem items de valor (ativos), por meio de um

ledger (livro-razão) comum distribuido, o qual cada participante possui uma cópia, e que seu conteúdo está em constante sincronia com os outros.

Eliminação de troca por intermediário e falta de confiança
Segurança e Integridade de processo
Transparência e imutabilidade
Simplificação de ecossistema
Descentralização

Até onde vai?

Internet do valor (dinheiro fluindo livremente como dados na Internet);

Blockchain-as-a-Service – BaaS

Mudanças estruturais no setor financeiro no médio e longo prazo.

Autonomia para os dispositivos de Internet das Coisas (Ex: lâmpada comprando energia de uma empresa de painéis solares).

Venda de bens culturais sem intermediários.

Possibilidades de aplicações

- Distribuição de benefícios e pensões, registro de transações imobiliárias, digital ID, Urna eletrônica. (Reino Unido, Suíça, Estônia)
- Mitigar o problema de falsificação e de roubo de celulares no mundo. (ITU)
- Monitoramento e rastreamento de uma cadeia de produção (ex: automóveis, equipamentos, vinhos,…).
- Controle de identidade dos dispositivos IoT.
- Aplicações de gestão de identidades.

Redes Criptografadas

“Entrando dentro de uma comunicação Digital”

Protocolos de comunicação

o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento.” (Kurose)

Protocolo de comunicação

Olá

Olá

Você viu o Homer?

Não vi!

Protocolo Humano

Solicitação de conexão

Resposta conexão

www.timao.com.br

Arquivo do site

Protocolo de redes de computadores

Imagem: pt.simpsons.wikia.com

Comunicação Digital

PROTOCOLOS DE REDES

PROTOCOLOS DE REDES

Protocolos

esta arquitetura de rede favorece o controle, não a liberdade, e esta característica reside nos protocolos técnicos que fazem destas conexões (Galloway)

Protocolos

“"Acima de tudo, a economia política do protocolo é o da gestão, modulação e controle. Técnica e politicamente a "sociedade de controle" emerge tanto de pesquisa cibernética como o faz a partir de um imperativo militar-industrial para a "governamentalidade" de sistemas de informação.” (Tracker, 1974)

Informações que não podem ser criptografadas em uma simples comunicação

Destinatário
(frente do envelope)

Remetente
(verso do envelope)

Analogia com a comunicação digital

Destinatário
(frente do envelope)

Endereço IP Destinatário

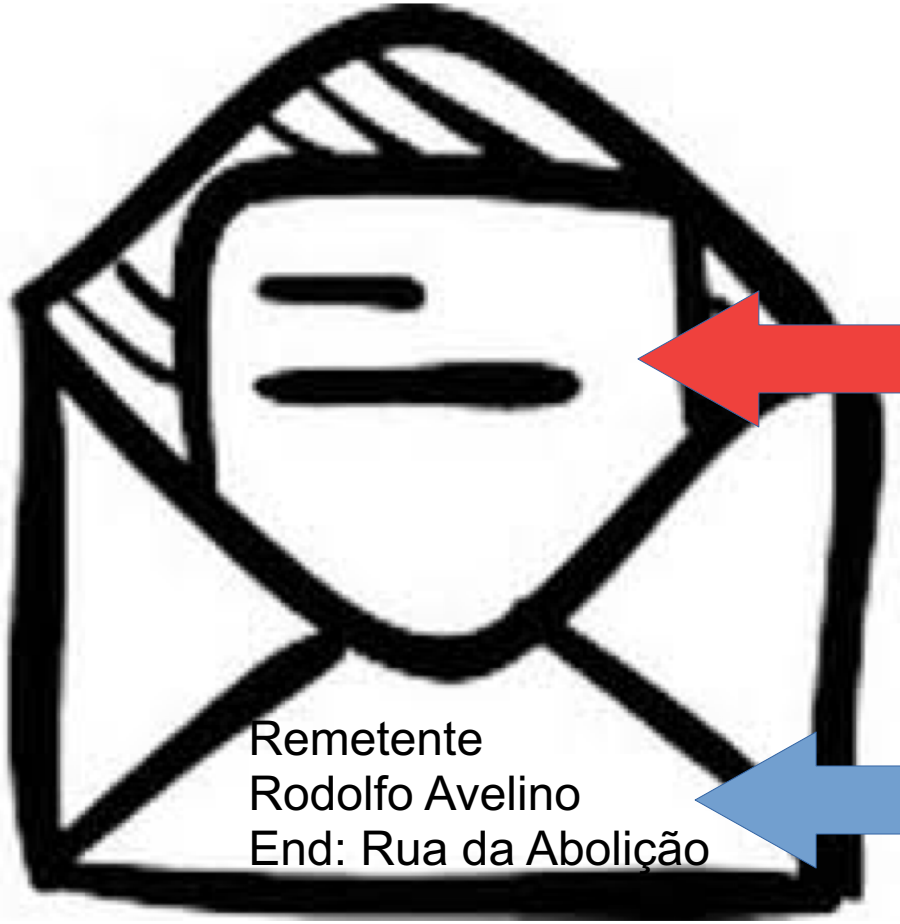
Remetente
(verso do envelope)

Endereço IP Origem

0101010101

METADATOS

0101010101

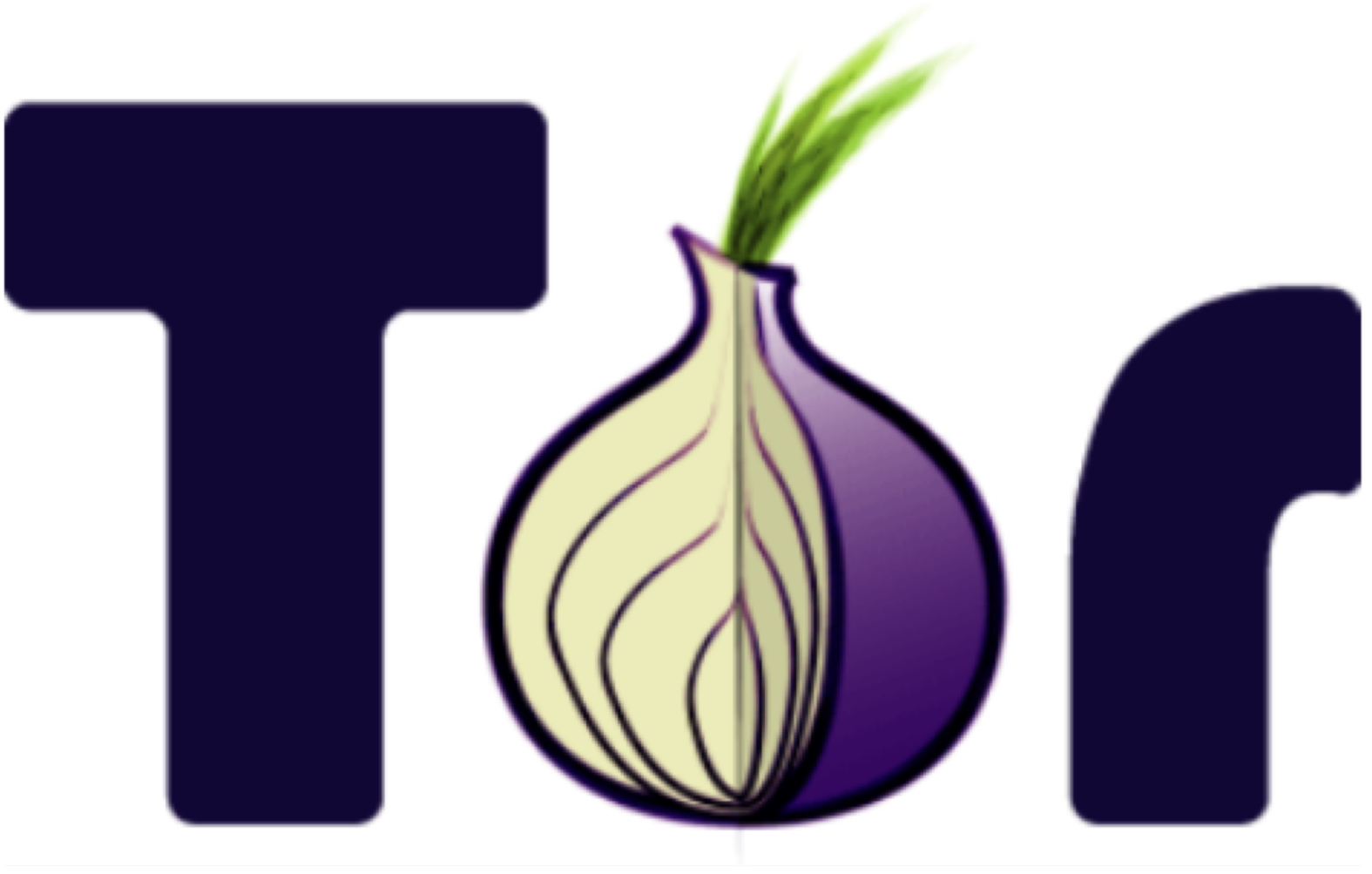


Conteúdo
Mensagem

Metadado

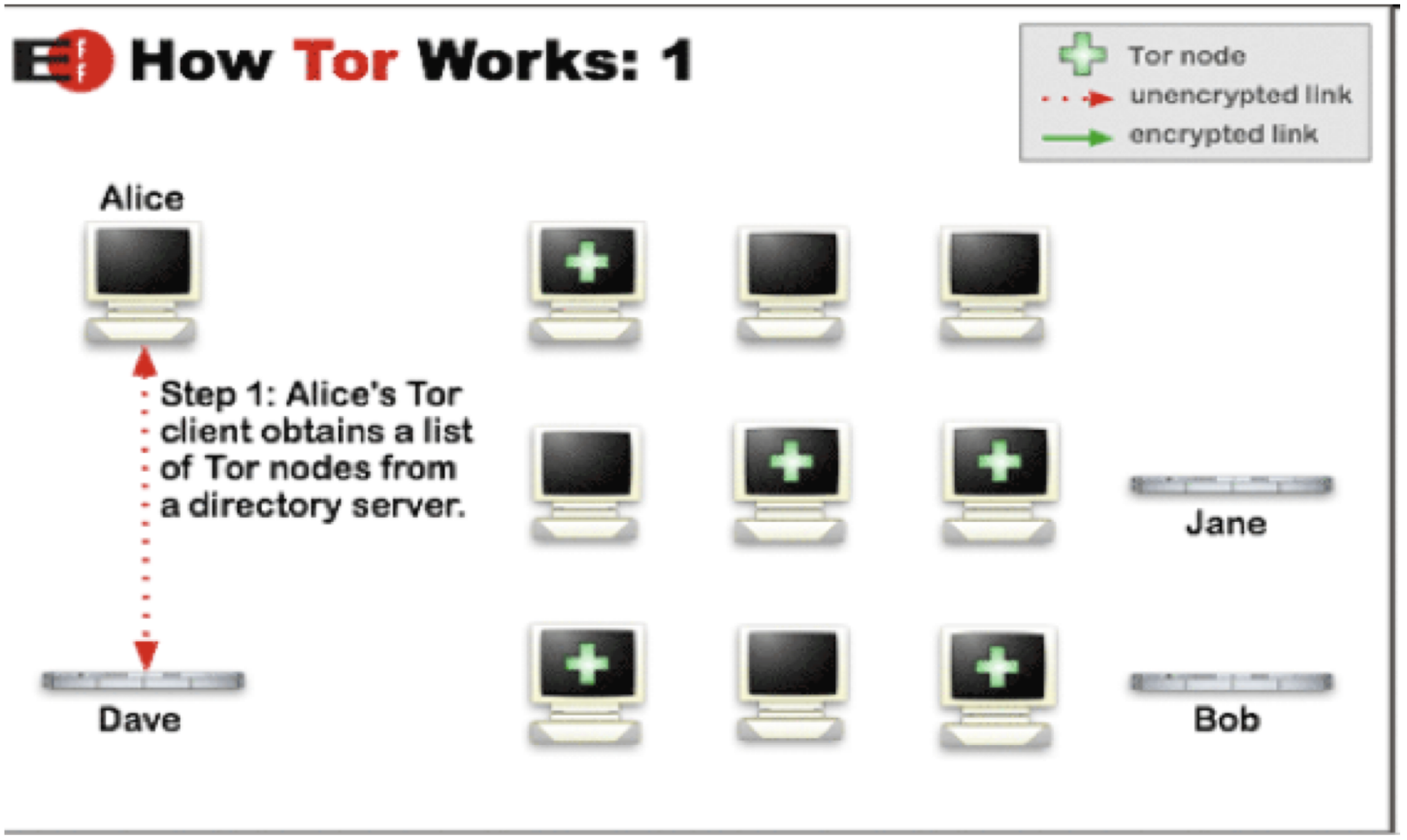
Problemas

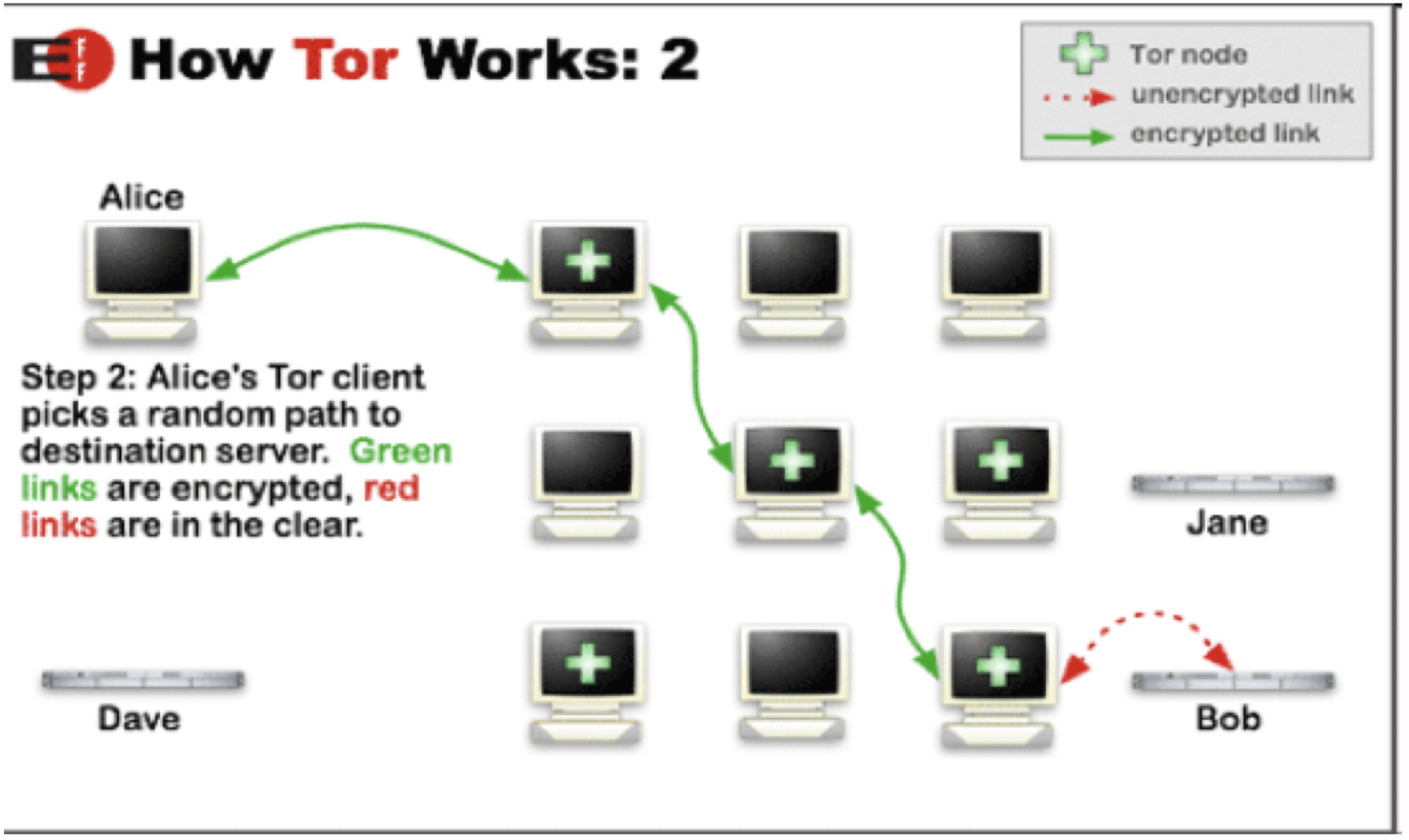
- A vigilância da Internet, como a análise de tráfego, revela a privacidade dos usuários.
- A criptografia não funciona, já que os cabeçalhos de pacotes ainda revelam muito sobre os usuários.
- O anonimato de ponta a ponta é necessário.
- Solução: uma rede anônima distribuída

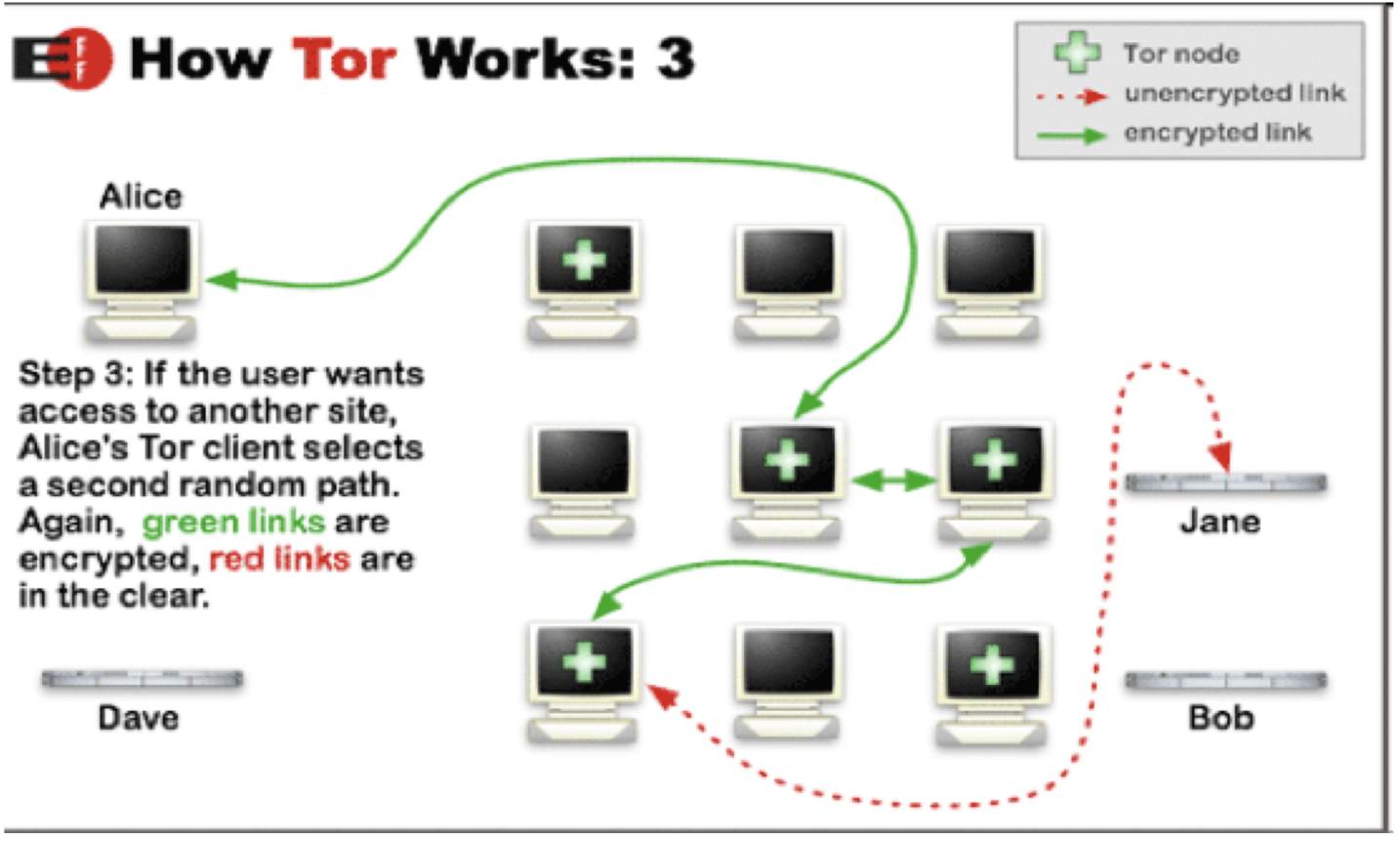

Tor

TOR

é um software livre e de código aberto que proporciona o anonimato pessoal ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade pessoal.


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Dave
Jane
Bob


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Bibliografia

Silveira, A. Sérgio. **Tudo Sobre Tod@s: redes digitais, privacidade e venda de dados pessoais.** São Paulo: Edicões SESC, 2017.

GALLOWAY, Alexander. **Protocol: how control existis after decentralization**. Cambridge: MIT Press, 2004.

KUROSE, J. F. e ROSS, K. **Redes de Computadores e a Internet.** - 5ª Ed., Pearson, 2010.

CONNECTing the Dots Outcome Document. UNESCO. http://unesdoc.unesco.org/images/0023/002340/234090e.pdf

Human Rights and Encrypt – UNESCO. http://unesdoc.unesco.org/images/0024/002465/246527e.pdf

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye.

Obrigado!

rodolfo.avelino@ufabc.edu.br