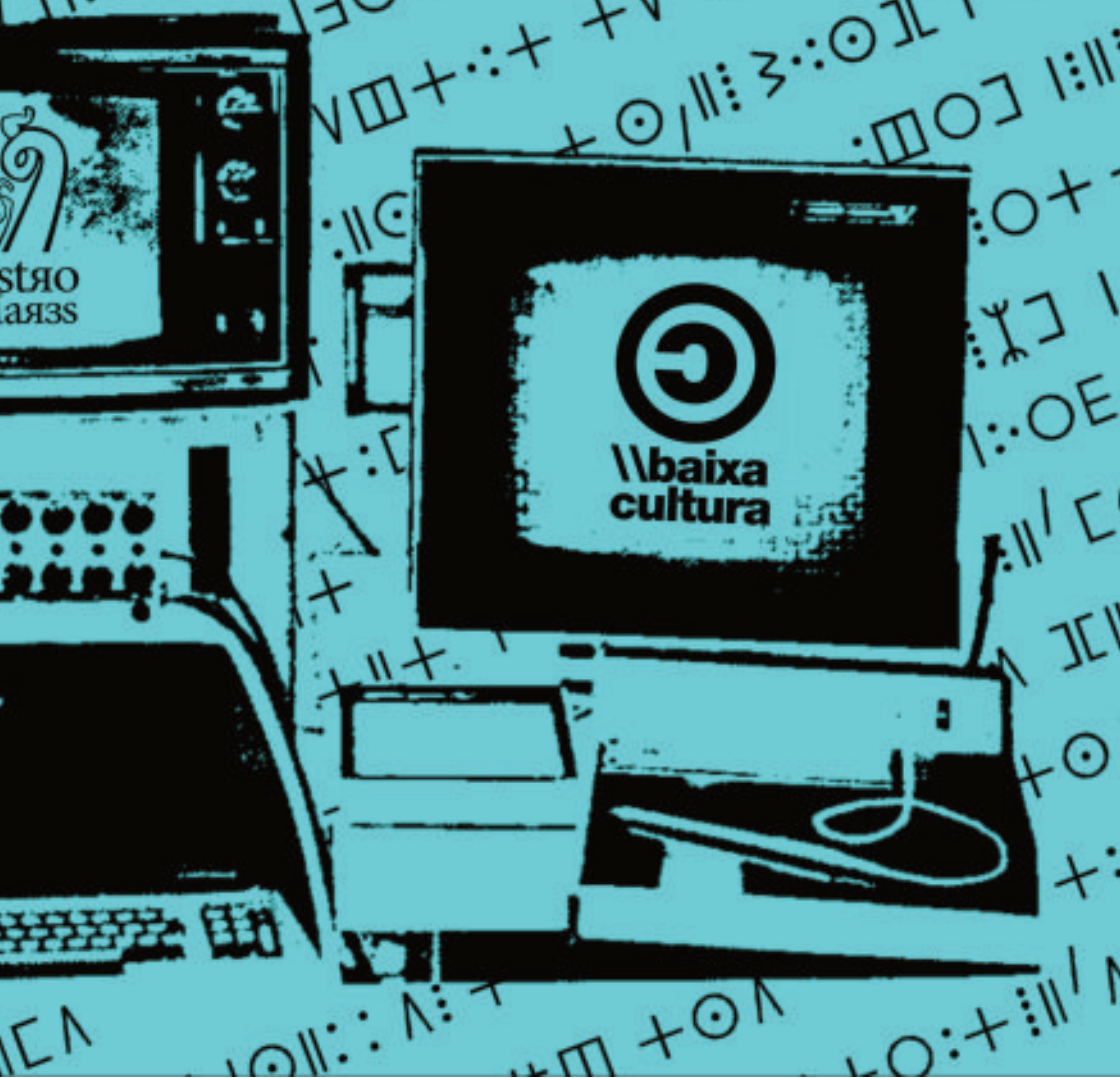
Manifestos Cypherpunks

Leonardo Foletto (org.)



Manifestos **Cypherpunks**

Leonardo Foletto (org.)

BaixaCultura
São Paulo – SP

Monstro dos Mares
Ponta Grossa – PR

Inverno de 2021

Manifestos Cypherpunks

Organização e introdução: *Leonardo Foletto*
Tradução: *Coletivo Cypherpunks*
Revisão da tradução: *Victor Wolffenbüttel*
Posfácio: *André Ramiro*
Diagramação e capa: *Baderna James*
Montagem e finalização: *abobrinha*
Revisão: *Raphael Sanz*

Monstro dos Mares
Divulgação Acadêmica Anárquica
Caixa Postal, 1560
Nova Rússia
Ponta Grossa, PR.
84071-981
https://monstrodosmares.com.br

Baixacultura
Cultura livre e contracultura digital
@baixacultura
info@baixacultura.org

https://baixacultura.org

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

M278 Manifestos cypherpunks / Organizador Leonardo Feltrin Foletto. – Ponta Grossa, PR: Monstro dos Mares, 2021.
60 p. : 14 x 21 cm

ISBN 978-65-86008-17-3

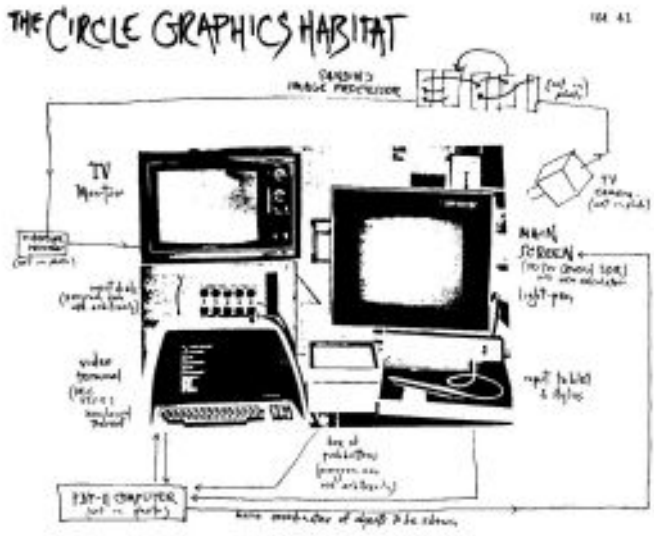
1. Internet – Aspectos sociais. 2. Hackers – Atividades políticas. 3. Liberdade de informação. I. Foletto, Leonardo Feltrin.
CDD 323.445

Elaborado por Maurício Amormino Júnior – CRB6/2422

Diagramação e impressão utilizando energia solar.

BaixaCultura é um laboratório de documentação, pesquisa e formação em cultura livre, (contra) cultura digital e tecnopolítica criado em 2008. *https://baixacultura.org*

A **Monstro dos Mares** se coloca como uma alternativa de publicação de baixíssimo custo para quem produz textos acadêmicos sobre epistemologias dissidentes que de alguma maneira se relacionam com as questões anárquicas de nosso tempo. *https://monstrodosmares.com.br*



Fonte: *Computer Lib/Dream Machines* (1974), zine publicado por Ted Nelson, p.41

O QUE É **CYPHERPUNK**?

Cypherpunks defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas. Criado no início dos anos 1990, o movimento teve destaque nas "criptoguerras" e após a censura da internet em 2011, na Primavera Árabe. O termo *cypherpunk* deriva de *cipher* (escrita cifrada) e *punk* e foi incluído no Oxford English Dictionary em 2006.†

† *Nota da edição:* Definição conforme ASSANGE, Julian. *Cypherpunks: liberdade e o futuro da internet*. Boitempo Editorial, 2015.

Sumário

INTRODUÇÃO

Criptografia em defesa da privacidade

Leonardo Foletto

Na década de 1970, o professor de literatura canadense Marshall McLuhan profetizou que o "novo mundo" criado pela tecnologia, com informação em abundância e "aldeias globais" amplamente conectadas e espalhadas pelo mundo, veria o fim de um dos direitos fundamentais da humanidade: a privacidade. "Eu discordava dele e dizia que ainda éramos capazes de manter silêncio sobre as coisas", afirmou em 2014 Derrick de Kerckhove[1], herdeiro da cadeira e do pensamento de McLuhan na Universidade de Toronto. "Ele dizia que não, que o fim da privacidade era como um tsunami: 'você pode nadar, mas não vai servir para nada'".

McLuhan construiu seu pensamento teórico *pop*, provocativo e amplamente difundido na mídia da época a partir de uma robusta pesquisa histórica e de uma coragem de apostar: dizia que os computadores estariam ligados em rede como a fase final das extensões do homem, chamada por ele de "simulação tecnológica da consciência", "pela qual o processo criativo do conhecimento se estenderá coletiva e carnalmente a toda a sociedade humana", como disse em seu clássico "*Understanding Media*" ("Os Meios de Comunicação Como Extensões do Homem", publicado no Brasil pela Cultrix desde 1969). Essa consciência tecnológica simulada e estendida a toda sociedade criaria um "novo mundo", não mais uma vila isolada, mas "a grande família humana em uma só tribo" – a aldeia global, um de seus conceitos mais conhecidos. Uma só tribo conectada e moldada pelas tecnologias

1 Fonte: https://baixacultura.org/o-fim-da-privacidade-e-a-etica-da-transparencia/

não teria mais lugar para o segredo: o direito à reserva de informações pessoais e da própria vida pessoal teria que ser embarcado nas tecnologias de comunicação para poder existir.

Corte para 2021: todos (ou quase todos) estamos conectados, tendo todas as nossas ações e o nosso tempo em frente a uma tela monitorados e quantificados por algumas empresas que, com esses dados – "o petróleo do Século XXI", numa expressão já tornada clichê –, ganham dinheiro e poder literalmente a *partir* da exposição de nossa privacidade. A ideia do *big data* – combinações infinitas de bancos de dados digitalizados diversos, estruturados para produzir novos significados – é uma *extensão do homem* mais potente e global do que McLuhan previu a partir das tecnologias de sua época, sobretudo as telecomunicações e a eletricidade.

Nesse cenário, como ainda pode ser possível falar de privacidade? Mais do que falar: como é possível cada um ainda proteger a sua privacidade? Kerckhove diz que não podemos mais nos proteger, o que seu antecessor talvez também diria. Ele não acredita em criptografia e defende, sim, uma "ética da transparência". "No lugar de tentar proteger sua privacidade com criptografia e senhas, que acabam quebradas mais cedo ou mais tarde, as pessoas deveriam passar a exigir dos governos e das empresas a mesma transparência a que suas vidas estão expostas".

Provavelmente, Kerckhove (muito menos McLuhan) não conheceu a fundo os *cypherpunks*, defensores da utilização da criptografia como meio para provocar mudanças sociais e políticas. Originários de uma vertente da cultura hacker mais afeita à ação política e libertária, em contraponto à outra mais ligada ao liberalismo empreendedor das *startups* do Vale do Silício, os *cypherpunks* surgem nos anos 1990 dizendo que a única maneira de manter a privacidade na era da informação é com uma criptografia forte. À pergunta sobre o fim da privacidade, eles replicam com um firme: *não.* E, para defendê-la, propõem o uso de tecnologias que respeitem o direito de cada um de proteger sua privacidade, tendo como elemento central a criptografia forte.

Ainda que o aspecto da "ética da transparência" seja uma questão importante também para os *cypherpunks* – vide as ações do Wikileaks, liderado por um dos mais conhecidos *hackers cypherpunks*, Julian Assange – a exigência de uma postura mais transparente dos governos vem junto de um trabalho de base de ensino da proteção individual e coletiva via criptografia. "Privacidade para os fracos, transparência para os poderosos", frase que virou lema do Wikileaks, indica de outra forma que exigir transparência de órgãos governamentais e particulares deve vir associado à proteção da privacidade de cada um contra a vigilância desses mesmos governos e empresas.

E, até hoje, o principal meio de se proteger da vigilância na internet é a partir do uso de criptografia. A "escrita escondida", presente desde a origem da palavra (do grego: *kryptós*, "escondido", e *gráphein*, "escrita") é uma técnica e uma prática de comunicação que visa proteger a segurança da mensagem da ação de terceiros, chamados na área de "adversários" (essa terminologia bélica representa bem a serventia militar que a criptografia teve ao longo de sua história). Os motivos da proteção de uma mensagem podem ser tantos quanto a criatividade humana quiser inventar: dos óbvios temas ligados à guerra aos não tão óbvios assuntos de amor, passando pela diplomacia e a competição, todos eles de alguma forma ligados ao "direito de ser deixado em paz" contida no entendimento comum de privacidade[2].

---

2 Há registros históricos muito antigos sobre o uso da criptografia; um dos primeiros remete a 1900 a.C., no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição. Alguns séculos depois, entre 600 a.C. e 500 a.C., os hebreus utilizavam a cifra de substituição simples (de fácil reversão e fazendo uso de cifragem dupla para obter o texto original), sendo monoalfabético e monogrâmica (os caracteres são trocados um a um por outros), e com ela escreveram o Livro de Jeremias. O chamado "Codificador de Júlio César" tornou-se popular (ainda hoje) como "Cifra de César", uma das técnicas mais clássicas de criptografia, em que o autor da cifragem troca cada letra por outra situada a três posições à frente no alfabeto. Uma simples ação que, diz a história, foi responsável por enganar muitos inimigos do Império Romano. Fonte: WIkipédia https://pt.wikipedia.org/wiki/Criptografia

Com a junção de computadores cada vez menores processando milhares de informações em cada vez menos tempo, e uma rede que une esses computadores todos ao redor do mundo, a criptografia tornou-se ainda mais importante. Não estamos mais falando apenas de situações raras ou estratégicas como, por exemplo, a proteção de trocas de bilhetes entre Imperadores e amantes no Império Romano, nem mesmo na cifragem de informações estratégicas de localização para ataques e defesas produzidas nos então rudimentares computadores da II Guerra Mundial. Agora são quase *todas* as informações da vida de uma pessoa que cruzam computadores potentes levados por nós a (quase) todos os lugares, que podem ser vistas por muita gente em qualquer canto do mundo a partir de outros computadores. São dados que, processados juntos com outras milhares de informações centralizadas em poucas empresas, extraem o suco da vida de alguém para então, de forma cada vez mais frequente, moldar nossos comportamentos a partir do endereçamento preciso de informação via plataformas digitais como *Facebook*, *Google*, *Instagram* ou *Twitter*.

Os textos presentes nestes *Manifestos Cypherpunks* são alguns dos primeiros alertas contra a vigilância massiva na era da internet. Foram escritos na época em que a rede mundial dos computadores ainda engatinhava, entre o final dos anos 1980 até meados dos 1990, por pessoas que conheciam a fundo alguns aspectos dos aparatos técnicos que faziam funcionar a rede e queriam nos fazer ficar atentos a eles. "Uma vez que uma infraestrutura de comunicações otimizada para a vigilância se torna arraigada, uma mudança nas condições políticas podem levar ao abuso desse poder recém-descoberto", escreveu em 1991 Philip R. Zimmermann, cientista da computação formado na Flórida que, na mesma ocasião, criou o PGP (*Pretty Good Privacy*), um programa de computador que utiliza criptografia assimétrica para proteger a privacidade do e-mail e dos arquivos armazenados no computador do usuário, software que é a base de muitos programas de criptografia ainda hoje.

Como outros textos desse período de nascimento da internet[3], alguns trechos desses manifestos podem soar premonitórios do que viria a ocorrer. A perseguição da criptografia pelo Estado, o que de fato ocorre neste 2021 no Brasil e em outros países, é um exemplo que já consta no segundo texto desta coletânea, "O Manifesto Criptoanarquista" (1993), de Timothy C. May, engenheiro eletricista que se tornou um dos mais reconhecidos *cypherpunks* assim que saiu da Intel, em 1986. "O estado tentará, é claro, desacelerar ou deter a disseminação dessas tecnologias, citando preocupações com a segurança nacional, o uso da tecnologia por traficantes de drogas e sonegadores de impostos, e temores de desintegração social. Muitas dessas preocupações serão válidas; a criptoanarquia permitirá que segredos nacionais sejam vendidos livremente e permitirá que materiais ilícitos e roubados sejam comercializados. Vários elementos criminosos e estrangeiros serão usuários ativos da CriptoNet. Mas isso não vai parar a propagação da criptoanarquia."

Como em May, também no terceiro texto desta publicação, "Manifesto Cypherpunk" (1993), de Eric Hughes, está presente um pensamento libertário, de desconfiança em relação ao Estado: "Não podemos esperar que governos, corporações ou outras organizações grandes e sem rosto nos concedam privacidade por benevolência. É para benefício próprio que falam de nós, e devemos esperar que eles vão falar. Tentar impedir a sua fala é lutar contra as realidades da informação. A informação não apenas quer liberdade, ela deseja ser livre", ecoando nesta última frase o primeiro princípio da ética hacker. Matemático e programador, Hughes, assim como os outros dois autores dos textos aqui, são filhos da cultura hacker dos Estados Unidos que ajudou a originar a internet, desenvolveu e potencializou o software livre e

---

3 "A Ideologia Californiana", de Richard Barbrook e Andy Cameron (1995), publicado como primeiro volume dessa coleção "Tecnopolítica", é um deles.

buscou tornar mais aberto o processo de produção das tecnologias para ajudar a deixá-las mais livres e autônomas. Com isso, mesmo que não fosse explícita a intenção, acabaram por politizar as tecnologias – ainda que a partir de um ponto de vista branco e masculino, o que, nos últimos anos, tem trazido diversas discussões dentro do movimento hacker e do software livre e aberto[4].

A resposta destes *Manifestos Cypherpunks* aqui publicados pode parecer até ingênua em 2021, segundo ano de pandemia do Novo Coronavírus, quando todos estamos mais necessitados de conexão e troca de dados para sobreviver ao isolamento necessário para não contrair a covid-19. Não deixa, também, de trazer ecos do solucionismo tecnológico, ideia muito em voga hoje em governos e empresas como a forma (supostamente) mais fácil de solucionar um problema sem precisar fazer política. [É ainda necessário dizer: a ideia de que uma tecnologia vai resolver todos os problemas de modo "fácil" frequentemente ignora os aspectos sociais, políticos e econômicos envolvidos na ação humana e na construção de aparatos tecnológicos].

Mas, como você lerá a seguir, as ideias presentes nos *Manifestos Cypherpunks* são, além de um alerta, um enfrentamento ao conformismo, que rejeita o "é melhor você se acostumar com o fim da privacidade" e acredita que o espalhamento da informação e do conhecimento sobre como funcionam os sistemas técnicos como a criptografia são ainda necessários para a transformação social. Também abordam a criptografia não apenas trazendo o uso de softwares como a grande solução para a defesa da privacidade, mas com uma discussão que envolve

---

4 Sobre estas questões, publicamos, no BaixaCultura, dois textos a partir da declaração machista de Richard Stallman, criador do software livre e também representante dessa mesma cultura hacker, em https://baixacultura.org/ja-passou-o-tempo-de-repensar-o-movimento-pelo-aberto-livre/ e https://baixacultura.org/isso-nao-e-um-manifesto-aberto-e-livre-em-reflexao/ .

questões filosóficas sobre como podemos agir, o que queremos preservar no mundo e o que temos direito a esconder. Como diz Hughes no último manifesto dessa coletânea, "devemos defender nossa própria privacidade se esperamos ter qualquer uma".

Leonardo Foletto *é jornalista e pesquisador, Doutor em Comunicação (UFRGS), editor do BaixaCultura e desta coleção "Tecnopolítica".*

POR QUE EU ESCREVI O **PGP** (1991)†

Philip R. Zimmermann

"Tudo que você fizer será insignificante,
mas é muito importante que você faça"
Mahatma Gandhi

É pessoal. É privado. E não é da conta de ninguém além da sua. Você pode estar planejando uma campanha política, discutindo seus impostos ou tendo um romance secreto. Ou você pode estar se comunicando com um dissidente político em um país repressivo. Seja o que for, você não quer que seu e-mail privado ou seus documentos confidenciais sejam lidos por qualquer outra pessoa. Não há nada de errado em afirmar sua privacidade. A privacidade é tão clichê quanto a Constituição.

O direito à privacidade é difundido implicitamente em toda a Declaração dos Direitos dos Cidadãos dos Estados Unidos (*Bill of Rights*). Mas quando a Constituição dos Estados Unidos foi emoldurada, os fundadores não viram necessidade de deixar explícito o direito à uma conversa privada. Isso teria sido bobo. Duzentos anos atrás, todas as conversas eram privadas. Se alguém estivesse ao alcance da voz, você poderia ir para trás do celeiro e conversar lá. Ninguém poderia ouvir sem o seu conhecimento. O direito à uma conversa privada era um direito natural, não apenas no sentido filosófico, mas no sentido das leis da física, dada a tecnologia da época.

---

† Parte do Guia do Usuário PGP original de 1991 (atualizado em 1999). Tradução: Coletivo Cypherpunks.com.br, disponível em https://cypherpunks.com.br/biblioteca/porque-eu-escrevi-o-pgp/ , com revisão de Victor Wolffenbüttel. O texto original, em inglês, está em https://nakamotoinstitute.org/why-i-wrote-pgp/ .

Mas com a chegada da era da informação, começando com a invenção do telefone, tudo mudou. A maioria das nossas conversas é conduzida eletronicamente agora. Isso permite que nossas conversas mais íntimas sejam expostas sem o nosso conhecimento. As chamadas de telefone celular podem ser monitoradas por qualquer pessoa com um rádio. O e-mail eletrônico, enviado pela Internet, não é mais seguro do que uma ligação por telefone celular. O e-mail está rapidamente substituindo o correio, tornando-se a norma para todos e não mais a novidade que era no passado.

Até recentemente, se o governo quisesse violar a privacidade dos cidadãos comuns, ele teria que gastar uma certa quantia de despesas e mão-de-obra para interceptar, abrir e ler cartas em papel. Ou ele teria que ouvir e possivelmente transcrever conversas telefônicas faladas, pelo menos antes de se tornar disponível a tecnologia de reconhecimento de voz automático. Esse tipo de monitoramento manual intensivo não era prático em grande escala. Isso só foi feito em casos importantes, quando parecia valer a pena. Era como pegar um peixe de cada vez, com um anzol e uma linha. Hoje, os e-mails podem ser verificados de forma rotineira e automática em busca de palavras-chave interessantes, em grande escala, sem detecção. É como pescar com redes de emalhar[†]. E o crescimento exponencial do poder computacional está fazendo a mesma coisa com o tráfego de voz.

Talvez você ache que seu e-mail é idôneo o suficiente para que a criptografia não seja necessária. Se você é realmente um cidadão seguidor da lei, sem nada a esconder, então por que você não envia suas cartas sempre em cartões postais? Por que não se submete a um teste de drogas quando solicitado? Por que exigir um mandado de busca se um policial quiser entrar em sua casa?

---

† *Nota da edição:* Um tipo de rede utilizada em artes de pesca passivas em que os peixes ou crustáceos ficam presos em suas malhas devido ao seu próprio movimento.

Você está tentando esconder alguma coisa? Se você esconder sua correspondência dentro de envelopes, isso significa que você deve ser um subversivo ou um traficante de drogas, ou talvez um louco paranóico? Os cidadãos seguidores da lei têm alguma necessidade de criptografar seus e-mails?

E se todos acreditassem que cidadãos seguidores da lei deveriam usar cartões postais para enviar correspondências? Se um não-conformista tentasse afirmar sua privacidade usando um envelope para suas cartas, isso levantaria suspeitas. Talvez as autoridades abrissem sua correspondência para ver o que ele está escondendo. Felizmente, não vivemos nesse tipo de mundo, porque todos protegem a maior parte das suas correspondências com envelopes. Portanto, ninguém levanta suspeitas afirmando sua privacidade com um envelope. Há segurança nos números. Analogamente, seria bom se todos usassem rotineiramente a criptografia para todos os seus e-mails, inocentes ou não, de modo que ninguém levantasse suspeitas ao afirmar a privacidade de seus e-mails com criptografia. Pense nisso como uma forma de solidariedade.

O Projeto de Lei 266 do Senado, de 1991, teve uma medida inquietante implicada nele. Se essa resolução não vinculante tivesse se tornado lei real, ela teria forçado os fabricantes de equipamentos de comunicações seguras a inserir "alçapões" especiais em seus produtos, para que o governo pudesse ler as mensagens criptografadas de qualquer pessoa. O projeto diz: "é de interesse do Congresso que os fornecedores de serviços de comunicações eletrônicas e os fabricantes de equipamentos de comunicações eletrônicas assegurem que os sistemas de comunicações permitam ao governo obter o conteúdo de texto simples de voz, dados e outras comunicações quando devidamente autorizado por lei." Foi este projeto de lei que me levou a publicar o PGP eletronicamente e de graça naquele ano, pouco antes de a medida ser derrotada, após os vigorosos protestos dos defensores das liberdades civis e grupos industriais.

A Lei de Assistência às Comunicações para a Segurança (CALEA), de 1994, determinou que as empresas telefônicas instalassem portas de interceptação remota em seus comutadores† digitais, criando uma nova infraestrutura de tecnologia para escutas telefônicas com apenas um clique, para que os agentes federais não precisassem mais sair e anexar grampos nas linhas telefônicas. Agora eles poderão se sentar em sua sede em Washington e ouvir seus telefonemas. Claro, a lei ainda exige uma ordem judicial para um grampo. Mas enquanto as infraestruturas tecnológicas podem persistir por gerações, as leis e políticas podem mudar da noite para o dia. Uma vez que uma infraestrutura de comunicações otimizada para a vigilância se torna arraigada, uma mudança nas condições políticas podem levar ao abuso desse poder recém-descoberto. As condições políticas podem mudar com a eleição de um novo governo, ou talvez mais abruptamente com o bombardeio de um prédio federal.

Um ano após a aprovação da CALEA, o FBI divulgou planos para exigir que as operadoras de telefonia construíssem em sua infraestrutura a capacidade de escuta simultânea de 1% de todas as chamadas telefônicas em todas as principais cidades dos EUA. Isso representaria um aumento de mais de mil vezes, em relação à capacidade anterior de números de telefones que poderiam ser interceptados. Nos anos anteriores, havia apenas cerca de mil escutas telefônicas nos Estados Unidos por ano, nos níveis federal, estadual e local combinados. É difícil entender como o governo poderia empregar juízes suficientes para assinar ordens de escuta suficientes para grampear 1% de todos os nossos telefonemas, muito menos contratar agentes federais suficientes para se sentar e ouvir todo o tráfego em tempo real.

---

† *Nota da edição:* Também conhecidos como *switches*, são dispositivos de interconexão usados para conectar computadores em uma rede formando o que é conhecido como rede local (LAN) e cujas especificações técnicas seguem o padrão conhecido como *Ethernet*.

A única maneira plausível de processar essa quantidade de tráfego é uma enorme aplicação orwelliana de tecnologia automatizada de reconhecimento de voz para analisar todas as palavras-chave, procurando por termos interessantes ou a voz de um determinado locutor. Se o governo não encontrar a meta na primeira amostra de 1%, as escutas telefônicas podem ser transferidas para outro 1%, até que a meta seja encontrada ou até que a linha telefônica de todos tenha sido verificada quanto ao tráfego subversivo. O FBI disse que eles precisam dessa capacidade para planejar o futuro. Este plano provocou tanta indignação que foi derrotado no Congresso. Mas o simples fato do FBI pedir por esses amplos poderes é revelador de sua agenda.

Avanços na tecnologia não permitirão a manutenção do status quo, no que se refere à privacidade. O status quo é instável. Se não fizermos nada, as novas tecnologias darão ao governo novas capacidades de vigilância automática, com as quais Stalin nunca poderia ter sonhado. A única maneira de manter a privacidade na era da informação é com uma criptografia forte.

Você não precisa desconfiar do governo para querer usar criptografia. Seu negócio pode ser interceptado por rivais empresariais, crime organizado ou governos estrangeiros. Vários governos estrangeiros, por exemplo, admitem usar seus sinais de inteligência contra empresas de outros países para dar às suas próprias corporações uma vantagem competitiva. Ironicamente, as restrições do governo dos Estados Unidos à criptografia nos anos 90 enfraqueceram as defesas corporativas dos EUA contra a inteligência estrangeira e o crime organizado.

O governo sabe o papel fundamental que a criptografia está destinada a desempenhar na relação de poder com seu povo. Em abril de 1993, o governo Clinton revelou uma nova e ousada iniciativa política sobre criptografia, que estava em desenvolvimento na Agência Nacional de Segurança (NSA) desde

o início do governo Bush†. O ponto central dessa iniciativa era um dispositivo de criptografia criado pelo governo, chamado de chip *Clipper*, contendo um novo algoritmo de criptografia secreto da NSA. O governo tentou incentivar a indústria privada a utilizá-lo em todos os seus produtos de comunicação segura, como telefones seguros, faxes seguros e assim por diante. A AT&T colocou o *Clipper* em seus produtos de voz seguros. A pegadinha: no momento da fabricação, cada chip *Clipper* é carregado com sua própria chave única, e o governo consegue manter uma cópia, colocada em custódia. Mas não se preocupe, o governo promete que usará essas chaves para ler seu tráfego apenas "quando devidamente autorizado por lei". Claro, para tornar o *Clipper* completamente eficaz, o próximo passo lógico seria proibir outras formas de criptografia.

O governo inicialmente alegou que o uso do *Clipper* seria voluntário, que ninguém seria forçado a usá-lo em vez de outros tipos de criptografia. Mas a reação pública contra o chip *Clipper* foi forte, mais forte do que o governo previa. A indústria de computadores monoliticamente proclamou sua oposição ao uso do *Clipper*. O diretor do FBI, Louis Freeh, respondeu a uma pergunta em uma conferência de imprensa em 1994 dizendo que, se *Clipper* não conseguisse apoio público, e grampos do FBI fossem excluídos por criptografia não controlada pelo governo, seu escritório não teria outra escolha senão buscar ajuda legislativa. Mais tarde, no rescaldo da tragédia de Oklahoma City†, o Sr. Freeh testemunhou perante o Comitê Judiciário do Senado que a disponibilidade pública de criptografia forte deveria ser limitada pelo governo (embora ninguém tenha sugerido que a criptografia tenha sido usada pelos responsáveis pelo bombardeio).

---

† *Nota da edição:* George H. W. Bush político, diplomata e empresário americano que foi presidente dos Estados Unidos de 1989 a 1993.

† *Nota da edição:* Explosão do Edifício Federal Alfred P. Murrah, no centro de Oklahoma City, Oklahoma, Estados Unidos, em 19 de abril de 1995, que matou pelo menos 168 pessoas e feriu mais de 680.

O histórico do governo não inspira a confiança de que eles nunca vão abusar de nossas liberdades civis. O programa COINTELPRO do FBI teve como alvo grupos que se opunham às políticas governamentais. Eles espionaram o movimento contra a guerra e o movimento pelos direitos civis. Grampearam o telefone de Martin Luther King. Nixon tinha sua lista de inimigos. Depois houve a bagunça do Watergate. Mais recentemente, o Congresso tentou aprovar leis restringindo nossas liberdades civis na Internet. Alguns elementos da Casa Branca de Clinton coletaram arquivos confidenciais do FBI sobre funcionários públicos republicanos para exploração política. E alguns promotores da justiça mostraram uma vontade de ir até os confins da Terra em busca de expor indiscrições sexuais de seus inimigos políticos. Em nenhum momento no século passado a falta de confiança pública no governo foi tão amplamente generalizada em todo o espectro político como é hoje.

Ao longo da década de 1990, eu percebi que, se quisermos resistir a essa tendência inquietante do governo de proibir a criptografia, uma medida que podemos aplicar é usar a criptografia, tanto quanto pudermos agora, enquanto ainda é legal. Quando o uso de criptografia forte se torna popular, é mais difícil para o governo criminalizá-la. Portanto, usar o PGP é bom para preservar a democracia. Se a privacidade for proibida, apenas os fora da lei terão privacidade.

Parece que a implantação do PGP deve ter funcionado, juntamente com anos de clamor público e pressão da indústria para diminuir os controles sobre a exportação. Nos últimos meses de 1999, o governo Clinton anunciou uma mudança radical na política de exportação para a tecnologia criptográfica. Eles jogaram fora todo o regime de controle de exportação. Agora, finalmente podemos exportar criptografia forte, sem limites superiores de resistência. Foi uma longa luta, mas finalmente vencemos, pelo menos em

relação ao controle de exportação nos EUA. Agora devemos continuar nossos esforços para implementar a criptografia forte, para amenizar os efeitos do aumento dos esforços de segurança na Internet de vários governos. E ainda precisamos consolidar nosso direito de usá-la domesticamente, apesar das objeções do FBI.

O PGP empodera as pessoas para que possam exercer sua privacidade com suas próprias mãos. Tem havido uma crescente necessidade social por isso, e é por isso que eu o escrevi.

Philip R. Zimmermann

Boulder, Colorado

Junho de 1991 (atualizado em 1999)

MANIFESTO **CRIPTOANARQUISTA** (1992)†

Timothy C. May

Cypherpunks do mundo,

Vários de vocês, na "reunião presencial de Cypherpunks", realizada ontem no Vale do Silício, pediram que o material distribuído nas reuniões estivesse disponível também eletronicamente para todo público da lista de Cypherpunks.

Aqui está "O Manifesto Criptoanarquista", que eu li na reunião de fundação, em Setembro de 1992. Ele remonta a meados de 1988 e foi distribuído a alguns "tecnoanarquistas" de mentalidade semelhante, na conferência "Crypto 88" e novamente na conferência "Hackers", este ano. Eu conversei mais tarde sobre isto com alguns hackers em 1989 e 1990.

Há algumas coisas que eu mudaria. Mas por razões históricas, deixarei o assunto assim. Alguns dos termos podem não ser familiares pra você. Espero que o Cripto Glossário que acabei de distribuir lhe ajude.

(Isto explica todos estes termos crípticos na minha assinatura!)

–Tim May

---

† *Tradução:* Coletivo Cypherpunks, disponível em https://cypherpunks.com.br/biblioteca/o-manifesto-criptoanarquista/ com revisão de Victor Wolffenbüttel. O original, em inglês, está aqui: https://nakamotoinstitute.org/crypto-anarchist-manifesto/

O MANIFESTO **CRIPTOANARQUISTA**

Timothy C. May – 1992

Um espectro está assombrando o mundo moderno, o espectro da cripto anarquia.

A ciência da computação está a ponto de fornecer a grupos e indivíduos a capacidade de se comunicar e interagir uns com os outros de maneira totalmente anônima. Duas pessoas podem trocar mensagens, conduzir negócios e realizar contratos digitais sem nunca conhecer o verdadeiro nome ou a identidade legal da outra parte. Interações em rede serão irrastreáveis, através de extensivo reencaminhamento de pacotes criptografados e caixas invioláveis, que implementam protocolos criptográficos com garantia quase perfeita contra qualquer adulteração. Reputações serão de importância central, muito mais importantes nas negociações do que nas avaliações de crédito de hoje. Esses desenvolvimentos irão alterar completamente a natureza da regulamentação governamental, a capacidade de taxar e controlar as interações econômicas, a capacidade de manter as informações em segredo e até mesmo alterar a natureza da confiança e da reputação.

A tecnologia para essa revolução – que certamente será tanto uma revolução social quanto econômica – já existia, em teoria, durante a última década. Os métodos são baseados em criptografia de chave pública, provas de conhecimento zero (*zero knowledge proofs*; ver Glossário ao final) interativos e vários protocolos de software para interação, autenticação e verificação. O foco, até agora, tem sido em conferências acadêmicas na Europa e nos EUA, monitoradas de perto pela Agência de Segurança Nacional (NSA). Mas só recentemente as redes de computadores e computadores pessoais atingiram velocidade suficiente para tornar as ideias realizáveis na prática. E os próximos dez

anos trarão velocidade suficiente para tornar as ideias economicamente viáveis e essencialmente imbatíveis. Redes de alta velocidade, caixas invioláveis, cartões inteligentes, satélites, transmissores, computadores pessoais e chips criptográficos, agora em desenvolvimento, serão algumas das tecnologias facilitadoras.

O estado tentará, é claro, desacelerar ou deter a disseminação dessas tecnologias, citando preocupações com a segurança nacional, o uso da tecnologia por traficantes de drogas e sonegadores de impostos, e temores de desintegração social. Muitas dessas preocupações serão válidas; a criptoanarquia permitirá que segredos nacionais sejam vendidos livremente e permitirá que materiais ilícitos e roubados sejam comercializados. Um mercado informatizado anônimo vai tornar possíveis mercados abomináveis para assassinatos e extorsões. Vários elementos criminosos e estrangeiros serão usuários ativos da CriptoNet. Mas isso não vai parar a propagação da criptoanarquia.

Assim como a tecnologia da impressão alterou e reduziu o poder das guildas medievais e a estrutura do poder social, os protocolos criptográficos também vão alterar fundamentalmente a natureza das corporações e as interferências do governo nas transações econômicas. Combinado com mercados de informação emergentes, a criptoanarquia criará um mercado líquido, para todo e qualquer material que possa ser colocado em palavras e imagens. E assim, como uma invenção aparentemente insignificante, como o arame farpado tornou possível o cercamento de vastas fazendas e territórios, alterando para sempre os conceitos de terra e direitos de propriedade na fronteira ocidental, também, a descoberta aparentemente menor de um ramo arcano da matemática se tornará o alicate que cortará o arame farpado em torno da propriedade intelectual.

Ergam-se, vocês não têm nada a perder a não ser as cercas de arame farpado!

MANIFESTO **CYPHERPUNK**
(1993)†

Eric Hughes

Privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é segredo. Um assunto privado é algo que não desejamos que o mundo inteiro saiba enquanto um assunto secreto é algo que ninguém quer que qualquer pessoa saiba. Privacidade é o poder de se revelar seletivamente ao mundo.

Se duas partes têm algum tipo de negociação, então cada uma tem uma memória de sua interação. Cada parte pode falar a partir de sua própria memória sobre isto. Como alguém poderia evitar isso? Pode-se aprovar leis contra ela, mas a liberdade de expressão ainda é fundamental para uma sociedade aberta, até mais que a privacidade; procuramos não restringir qualquer discurso. Se muitas partes falam juntas no mesmo fórum, cada uma pode falar com todos os outros e agregar conhecimento sobre indivíduos e outras partes. O poder das comunicações eletrônicas permitiu tal conversação em grupo, e ela não vai embora apenas porque poderíamos querer.

Uma vez que desejamos privacidade, devemos garantir que cada parte de uma transação tenha conhecimento apenas do que é diretamente necessário para essa transação. Uma vez que qualquer informação pode ser falada, devemos garantir que revelamos o mínimo possível. Na maioria dos casos, a identidade pessoal não é saliente. Quando eu compro uma revista em uma loja e entrego dinheiro para o funcionário, não há necessidade

† *Tradução:* Coletivo Cypherpunks, disponível em: https://cypherpunks.com.br/biblioteca/o-manifesto-cypherpunk/ com revisão de Victor Wolffenbüttel. O original, em inglês, está em https://nakamotoinstitute.org/cypherpunk-manifesto/ .

de saber quem eu sou. Quando peço ao meu provedor de e-mail para enviar e receber mensagens, ele não precisa saber a quem estou falando ou o que estou dizendo ou o que os outros estão dizendo para mim. Meu provedor só precisa saber como obter a mensagem lá e quanto eu devo-lhes em taxas. Quando minha identidade é revelada pelo mecanismo subjacente da transação, não tenho privacidade. Eu não posso aqui me revelar seletivamente; *sempre* devo me revelar.

Portanto, a privacidade em uma sociedade aberta requer sistemas de transações anônimas. Até agora, o dinheiro foi o principal sistema. Um sistema de transação anônima não é um sistema de transação secreta. Um sistema anônimo capacita os indivíduos a revelar sua identidade quando desejado e somente quando desejado. Esta é a essência da privacidade.

Privacidade em uma sociedade aberta também requer criptografia. Se eu disser algo, quero que seja ouvido apenas por aqueles para quem eu pretendo dizê-lo. Se o conteúdo do meu discurso está disponível para o mundo, eu não tenho privacidade. Criptografar é indicar o desejo de privacidade, e criptografar com criptografia fraca é não indicar muito desejo de privacidade. Além disso, revelar a identidade com certeza quando o padrão é anonimato requer a assinatura criptográfica.

Não podemos esperar que governos, corporações ou outras organizações grandes e sem rosto nos concedam privacidade por benevolência. É para benefício próprio que falam de nós, e devemos esperar que eles vão falar. Tentar impedir a sua fala é lutar contra as realidades da informação. A informação não apenas quer liberdade, ela deseja ser livre. As informações se expandem para preencher o espaço de armazenamento disponível. A informação é a prima mais jovem e mais forte do rumor; a informação é rápida com os pés, tem mais olhos, sabe mais, e compreende menos do que o rumor.

Devemos defender nossa própria privacidade se esperamos ter qualquer uma. Temos de nos unir e criar sistemas que permitam transações anônimas. As pessoas têm defendido sua própria privacidade por séculos com sussurros, escuridão, envelopes, portas fechadas, apertos de mão secretos e mensageiros. As tecnologias do passado não permitiam a privacidade forte, mas as tecnologias eletrônicas sim.

Nós, os Cypherpunks, estamos dedicados a construir sistemas anônimos. Estamos defendendo nossa privacidade com criptografia, sistemas anônimos de encaminhamento de e-mails, assinaturas digitais e dinheiro eletrônico.

Cypherpunks escrevem códigos. Sabemos que alguém tem de escrever software para defender a privacidade, e uma vez que não podemos ter privacidade a menos que todos nós tenhamos, vamos escrevê-lo. Nós publicamos nosso código para que nossos companheiros Cypherpunks possam praticar e brincar com ele. Nosso código é gratuito para todos, em todo o mundo. Não nos importamos muito se você não aprovar o software que escrevemos. Sabemos que o software não pode ser destruído e que um sistema amplamente disperso não pode ser desligado.

Os Cypherpunks não se importam com regulamentos sobre a criptografia, pois ela é um ato privado. O ato de cifrar, na verdade, remove informações do domínio público. Mesmo as leis contra a criptografia alcançam apenas a fronteira de uma nação e o braço de sua violência. A criptografia se espalhará inelutavelmente por todo o globo junto com os sistemas de transações anônimas que ela possibilita.

Para que a privacidade seja generalizada, ela deve fazer parte de um contrato social. As pessoas devem se unir e juntas implementar esses sistemas para o bem comum. A privacidade se estende tanto quanto a cooperação entre seus companheiros na sociedade. Nós os Cypherpunks procuramos perguntas e preocupações

e esperamos que possamos engajar nossos companheiros de sociedade para que não nos desapontemos. Não seremos, no entanto, afastados do nosso curso porque alguns podem discordar dos nossos objetivos.

Os Cypherpunks estão ativamente empenhados em tornar as redes mais seguras para a privacidade. Vamos avançar juntos.

Avante.

Eric Hughes
<hughes@soda.berkeley.edu>
9 de Março de 1993

POSFÁCIO

Retrospectiva e expectativa Cypherpunk

André Ramiro

Com mais de trinta anos da sua gênese – uma confluência de ameaças de mecanismos regulatórios sobre a exportação de criptografia, utopias californianas[1] que resistiam a ensaios de políticas de vigilância (que se materializariam no futuro próximo) e uma sequência de encontros entre engenheiros de software e hardware influenciados por escritos tecno-libertários – o ideal dos *cypherpunks* germinaria sobre gerações de criptógrafos, programadores e ativistas. O movimento irá compor um verdadeiro *sistema* de natureza tecno-social que ganharia uma *elasticidade* em diferentes contextos sociopolíticos desde o fim da década de 80 até os dias de hoje.

Isso porque, ainda que *cypherpunk* significasse inicialmente um grupo de pessoas podemos expandir sua simbologia para além da qualidade pessoal e agregar diferentes formas de "ação política". Quer dizer, tecnologias podem ser cypherpunks, como o *The Onion Router* (Tor), o *Pretty Good Privacy* (PGP) ou o *WikiLeaks*; articulações sociais podem ser *cypherpunks*, como as criptofestas em dezenas de localidades do mundo e as diversas mobilizações da sociedade civil de defesa dos direitos conexos à

1 É interessante pensar como o libertarianismo *cypherpunk* dialoga, ainda que pontualmente, com o que Richard Barbrook e Andy Cameron chamaram de "ideologia californiana". Timothy May, por exemplo, foi leitor de Ayn Rand e refletia, em alguns posicionamentos políticos, parte da sua filosofia centrada em um certo individualismo. Ver GREENBERG, Andy. *This machine kills secrets*: how WikiLeakers, cypherpunks, and hacktivists aim to free the world's information. Dutton, 2012.

criptografia na rede; e pessoas podem ser *cypherpunks* através de ações cipher-ativistas, como aqueles/as que se dedicam, em redes colaborativas, a oferecer oficinas sobre o uso de ferramentas de criptografia, organizações que defendem a criptografia em processos judiciais ou indivíduos que alimentam o *GitHub* com linhas de código que tornam mais resilientes arquiteturas de segurança com criptografia.

Se "*cypherpunks* estão ativamente engajados em fazer redes mais seguras para a privacidade", como diz Hughes no terceiro texto dessa coletânea, seria possível ainda arriscar e dizer que certas legislações também carregam uma dimensão *cypherpunk*, a exemplo do Marco Civil da Internet (MCI), um modelo de regime legal sobre o uso da Internet no Brasil, construído democraticamente, em longo processo consultivo com distintos setores da sociedade e cuja fundação sedimenta o direito à liberdade de expressão, a privacidade e o sigilo das comunicações na rede. Não à toa, a observação das regras do MCI[2] tem sido fundamental para afastar as tentativas de bloqueio de aplicativos com criptografia ponta-a-ponta no país.

---

2 Bem como do Decreto que o regulamenta (Decreto nº 8771/2016), que estabelece a criptografia como recurso necessário à garantia da inviolabilidade dos dados pessoais sob responsabilidade de provedores de conexão e aplicação.

Cypherpunks para tornar o big brother obsoleto

Todas essas expressões, no entanto, carregam transversais que são invariáveis: defendem a criptografia e os sistemas descentralizados. Esses elementos estão também nas ideias iniciais de David Chaum – o "profeta sem intenção" dos *cypherpunks* dos anos 90. Em um artigo chamado "*Security Without Identification: Transaction Systems to Make Big Brother Obsolete*" (1985), conseguimos mapear boa parte da crítica à vigilância governamental – e às múltiplas faces dos mercados de dados pessoais cujo saldo resulta em uma inibição galopante do indivíduo e da coletividade – que será explorada nos manifestos publicados aqui[3]. Timothy May, então recém-ex-funcionário da Intel[4], irá dar tração às ideias de Chaum com o primeiro dos manifestos *cypherpunks*, o Manifesto Criptoanarquista, o segundo desta coletânea.

Na visão de Tim May, a criptografia de chave pública foi tão importante para a virada do século XXI, em termos de revolução comunicacional, quanto a invenção da prensa de Gutenberg foi no século XV. Da mesma forma que a difusão de conhecimento possibilitada pela prensa potencializou a desestruturação do modelo de retenção e silenciamento de informações característicos do poder medieval, a criptografia seria, igualmente,

---

3 "A computação está afastando os indivíduos de sua habilidade de monitorar e controlar as formas que informações sobre eles são utilizadas. (...) Um alicerce está sendo posto para uma sociedade do dossiê, na qual computadores podem ser usados para inferir sobre o estilo de vida, os hábitos, a localização e associações dos indivíduos a partir de dados coletados em transações de consumo ordinárias" (trecho em tradução livre).

4 Conta-se que Tim May, após sua saída da Intel e já engajado com a guerrilha em defesa da privacidade, irá se apropriar do famoso logo da empresa (*Intel Inside*) para criar o que seria um dos primeiros *memes* anti-vigilantistas: em diversas lojas de eletrônicos da região, irá colar adesivos com a logo "Big Brother Inside".

o contraponto da escalada de poder do Estado com a aceleração da computação. De fato, para os estudos de vigilância dos finais da década de 80, a centralização do computador enquanto ferramenta de administração pública completaria o projeto panóptico de Jeremy Bentham de duas maneiras: expondo o comportamento do público e tornando opacos os aparatos de vigilância.[5]

No ínterim do aprofundamento das preocupações sobre a erosão da privacidade, os manifestos de May e Eric Hughes foram sintomáticos, respectivamente, do presságio e da reação às "criptoguerras" (como viriam a ficar conhecidas as disputas em torno da criptografia notadamente na década de 90, mas com diversas renovações contemporâneas): em 1988, ano da primeira aparição do Manifesto Criptoanarquista[6], já era densa a proximidade dos riscos aos direitos refletidos em regulações restritivas à criptografia; em 1993, o "Manifesto Cypherpunk" já mobilizava um repertório de reação a políticas públicas e teorizava, ainda que implicitamente, sobre o direito à privacidade e à proteção de dados[7]. Coincidentemente, no mesmo ano era publicado no Brasil o ensaio "Sigilo dos dados: o direito à privacidade e os limites da função fiscalizadora do Estado", de Tércio Sampaio Ferraz Júnior, um marco teórico na sedimentação do direito ao sigilo das comunicações no país.

---

5 LYON, David. *9/11, Synopticon, and Scopophilia:* Watched and Being Watched. University of Toronto Press, 2005. p.44.

6 Conta-se que Tim May distribuíra fotocópias com os primeiros rascunhos do Manifesto em uma conferência sobre criptografia em Santa Barbara, em 1988, onde praticamente ninguém lhe dava atenção. Não se davam conta de que recebiam escritos que ficariam para a história. Ver Andy Greenberg. *Op cit.* p. 72-74.

7 FERRAZ JR. Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*, USP, Vol. 88. p. 447-448. Disponível em https://revistas.usp.br/rfdusp/article/view/67231.

A conjuntura político-tecnológica de 1993, ironicamente, dará o pontapé inicial ao *Clipper Chip*, proposta da *National Security Agency* (NSA) para prever *backdoors*[8] nos produtos destinados à comunicação nos Estados Unidos, o que apenas confirma que as "antenas" do *cypherpunks* estavam sintonizadas na frequência certa. Esse específico recorte histórico também é especialmente importante para uma possível "arqueologia do ciberativismo": algumas das pioneiras organizações focadas na defesa dos direitos digitais têm seu berço de trabalho na incidência política contra o *Clipper Chip*, como a *Electronic Privacy Information Center* (EPIC) e a *Electronic Frontier Foundation* (EFF) – fundada, entre outras pessoas, por John Gilmore, figura notória do núcleo original de *cypherpunks*.

---

8 "Porta dos fundos" em sistemas criptográficos previstos para permitir o acesso ao conteúdo das comunicações para autoridades governamentais.

A criptografia forte[9] desestabilizaria, portanto, históricas e culturais estruturas estatais de vigilância. Por isso, as ininterruptas tentativas de inserir "desvios" em sistemas criptográficos[10] sugerem ser mecanismos governamentais que buscam manter um *status quo* sociopolítico através da manutenção do monitoramento da sociedade para neutralizar potenciais transformações sociais que, naturalmente, dependem de canais de comunicação privados para se manifestarem.

Por essas e outras razões, no balanço que Phil Zimmerman[11] faz sobre a atmosfera da década de 90 que ensejou o PGP e as expressões *cypherpunks*, relata a larga e distribuída desconfiança pública em relação ao Estado devido à banalização de grampos em, por exemplo, lideranças do movimento anti-guerra e por direitos civis, algo também amplamente refletido em autores, como Frank Donner ou Gary T. Marx[12], que mapearam a capilaridade

---

9 Aquela que não permite acesso ao conteúdo encriptado mesmo diante de uma eventual ordem judicial.

10 Diferentes formas de superar o sigilo criptográfico são sucessivamente propostas na busca por um "desvio": achar a chave, adivinhar a chave, forçar a entrega da chave, explorar uma vulnerabilidade, acessar o texto antes de ser cifrado ou encontrar uma cópia do texto. Ver, por exemplo, a taxonomia proposta por KERR, Orin; SCHNEIER, Bruce. Encryption Workarounds. 106 *Georgetown Law Journal* 989, 2018. Pág 8.

11 É interessante que a associação de Zimmerman com o espectro *cypherpunk* só se tornou mais orgânica quando o PGP foi carimbado (inclusive pela mídia) como contraponto tecnológico ao *Clipper Chip*. Antes disso, a postura mais branda, menos anárquica ou anti-governo de Zimmerman o afastava, ideologicamente, do grupo original. Ver LEVY, Steven. *Crypto:* how the code rebels beat the Government, saving privacy in the digital age. Penguin Books, 2002.

12 Ver DONNER, Frank. *The Age of Surveillance:* The Aims and Methods of America's Political Intelligence System. Vintage Press, 1981; e MARX, Gary T. *Undercover:* Police Surveillance in America. University of California Press, 1988. Uma realidade não exatamente diferente do que acontece no Brasil: em 2009, o país foi condenado pela Corte Interamericana de Direitos Humanos pelos grampos ilegais em nas comunicações de lideranças ligadas ao Movimento Sem Terra, no Paraná; em 2020, foi revelada a criação de dossiês, sob responsabilidade do Ministério da Justiça, sobre pessoas ligadas ao movimento antifascista, além da infiltração de agentes da Agência Brasileira de Inteligência (ABIN) em universidades públicas.

dos aparatos de vigilância, infiltração e interceptações telefônicas nos Estados Unidos. O movimento *cypherpunk*, portanto, pode ser encarado como uma ação "anti-sistema" (aquele promotor de injustiças derivadas da concentração de poder corporativo e governamental) e, antes de querer manter uma "ordem anterior" à Internet, é propositivo em se permitir sonhar com uma mudança estrutural necessária aos sistemas de dispositivos conectados em detrimento da expansão do tráfego de dados pessoais.

Não por acaso, o termo "*cypherpunk*" merece uma designação própria na taxonomia proposta por Arvind Narayanan[13] para classificar aplicações da criptografia tendo em vista suas finalidades. A classificação reuniria categorias como "*crypto for security*", geralmente destinada à proteção de transações eletrônicas e relacionada ao desenvolvimento econômico online; e "*crypto for privacy*", que se ramificaria em "*pragmatic crypto*", aquela que prevê a manutenção de um nível de privacidade de uma realidade pré-digital, e "*cypherpunk crypto*", aquela que vê na criptografia um eixo tecnológico de transformação social e política inexorável.

---

13 NARAYANAN, Arvind. *What Happened to the Crypto Dream?*, Part 1. IEEE Computer and Reliability Societies, 2013.
Disponível em https://is.gd/2bZW4s .

A criptografia, portanto, desempenha uma função de "embargo" tecnológico ao acesso não autorizado ou abusivo às comunicações e aos dados. Isso faz dela não somente um instrumental necessário ao exercício de direitos, mas a entrelaça, para além da formulação de políticas públicas, com uma responsabilidade social do desenvolvimento tecnocientífico.

No ensaio "*The Moral Character of Cryptographic Work*", Phillip Rogaway, professor da Universidade da Califórnia, remonta ao significado do Projeto Manhattan e às posteriores reflexões sobre as justificativas que norteiam a moral latente do trabalho científico para re-enquadrar o papel dos criptógrafos em uma era pós-Snowden. Durante a Segunda Guerra, físicos e matemáticos aderiram ao uma estratégia política supostamente necessária à sustação do holocausto e do expansionismo nazista através da participação em projetos de fabricação de armas de destruição em massa. Da mesma forma, após os atentados de 11 de setembro de 2001, a comunidade de cientistas da computação, incluindo criptógrafos, cederam a um patriotismo atiçado por um novo projeto político, dessa vez da "guerra ao terror".

Como resultado, se uma revisão foi operada pela comunidade de físicos após o trauma histórico de Hiroshima e Nagasaki, com uma clara sinalização ao humanismo através do Manifesto Russell-Einstein[14] ou com a crise existencial de Robert Oppenheimer[15], os criptógrafos

---

14 "Precisamos pensar de uma nova forma. Precisamos aprender a nos perguntar não que passos podem ser dados para dar a vitória militar a qualquer grupo que preferirmos, pois não existem mais tais passos. A questão que precisamos nos perguntar é: quais passos podem ser dados para impedir uma corrida militar a partir da qual os problemas serão desastrosos para todos?" (trecho em tradução livre). BORN, Max e outros. *The Russell-Einstein Manifesto*. Student Pugwash Michigan, 1955. Disponível em http://umich.edu/~pugwash/Manifesto.html .

15 ANDERSON, Tim. *Oppenheimer's Dilemma*. Stanford University. 2016. Disponível em http://large.stanford.edu/courses/2016/ph241/anderson1/ .

haveriam de revisitar a dimensão sociopolítica de seu campo. Estariam, portanto, na linha de frente da resistência necessária ao exercício de direitos humanos em uma crescente disputa tecnológica que acompanha a digitalização dos espaços cívicos e políticos na Internet.

Em grande medida, essa provocação já habitava o espectro ideológico dos *cypherpunks*. E como a recente história do ciberativismo vem demonstrando, não são os criptógrafos, mas os *cypherpunks* que defendem com unhas e dentes o emprego de criptografia forte em sistemas de comunicação e armazenamento de dados, conscientes – e promotores – de dimensões tecno-sociais que vão além dos desafios matemáticos da criptografia.

É interessante pensar como o Brasil acabou se tornando um terreno fértil para um movimento *cipher-ativista* consideravelmente duradouro. Assim como em outros países, carregamos uma bagagem judicial-legislativa de ameaças ao pleno uso de criptografia forte, como vem ocorrendo na Austrália, na Índia ou nos Estados Unidos. Distintos Projetos de Lei[16] e decisões judiciais, nos últimos anos, formam um mosaico das diferentes formas como o Estado brasileiro demonstrou seu incômodo com os espaços de privacidade alcançados com o uso massificado de criptografia ponta-a-ponta. Como efeito colateral, foi desencadeado um processo de amadurecimento técnico e legal sobre as relações entre criptografia, segurança do ecossistema da Internet e promoção dos direitos digitais.

Entre 2015 e 2016, quatro decisões judiciais ordenaram o bloqueio do WhatsApp em território nacional, das quais três foram efetivamente cumpridas (com efeitos na infraestrutura de conectividade e acesso à aplicação percebidas em outros países, como no Chile e na Argentina). Em linhas gerais, entendiam que a criptografia não poderia desafiar ordens judiciais que demandassem pelo acesso a comunicações no âmbito de uma investigação criminal. Todas as decisões foram eventualmente revertidas em instâncias judiciais superiores e, em 2017, o Supremo Tribunal Federal (STF)[17] realizou Audiência Pública para ouvir especialistas e unificar entendimento sobre a situação da criptografia forte no país.[18]

---

16 Como o Projeto de Lei nº 9.808/2018, que pretendia modificar o Marco Civil da Internet para conferir aos delegados de polícia o poder de, sem necessidade de ordem judicial, demandar a um provedor de serviços a chave para decriptar comunicações que julgassem suspeitas.

17 A Ação Direta de Inconstitucionalidade (ADI) nº 5527 e a Ação de Descumprimento de Preceito Fundamental (ADPF) nº 403 foram propostas no STF para resolver, cada uma a sua maneira, o entendimento das decisões de instâncias inferiores que se multiplicavam e traziam certa insegurança jurídica aos usuários e às plataformas.

Uma diversidade de representações de professores universitários, pesquisadores e organizações não-governamentais se manifestaram na Audiência (e fora dela, através de campanhas ou publicações) contra qualquer decisão judicial ou política pública que busque limitar a segurança da informação e os direitos conexos e dependentes do pleno emprego da criptografia. Essa conjuntura despertou, a meu ver, um verdadeiro efeito *cypherpunk* na comunidade brasileira de defensores dos direitos humanos, advogados, ativistas da democratização da comunicação, cientistas da computação, engenheiros de software, entre tantas outras áreas da atuação política resultantes da equação entre desenvolvimento tecnológico, defesa da democracia e segurança da rede.[19]

Mas ainda que tenhamos avançado em mobilização, incidência política e produção de conhecimento, essas tensões parecem perdurar tanto quanto se mantiveram presentes condições socioeconômicos desiguais, sobretudo onde o discurso populista da "lei e ordem" – especialmente em forma de políticas de vigilância – alcança amplas parcelas da população e projetam lideranças autoritárias. O legado ideológico dos *cypherpunks*, cristalizado nos seus manifestos, deve percorrer os laboratórios de produção tecnocientífica, as instituições de pesquisa sociais, os centros de formulação de políticas públicas e as organizações da sociedade civil. Cabe a nós mantermos o arco teso – e o fluxo de comunicações e dados encriptado.

***André Ramiro** é um dos fundadores e diretor do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Pesquisador de criptografia, vigilância e direito, é fellow da Derechos Digitales (Chile) e mestrando em Ciências da Computação na UFPE.*

---

18 SUPREMO TRIBUNAL FEDERAL. Audiência Pública sobre a Ação Direta de Inconstitucionalidade nº 5.527 e a Ação de Descumprimento de Preceito Fundamental nº 403. Supremo Tribunal Federal. 2017. Disponível em https://is.gd/nid5Ds .

19 Encontrando paralelo no espírito de luta pelos direitos civis na década de noventa nos Estados Unidos – onde se colocam historicamente os manifestos – entendo que o movimento *cypherpunk* no Brasil se relaciona, antes, com a oposição a políticas que ameaçam a robustez de sistemas criptográficos e o conjunto de direitos a eles conexos em nome de maiores capacidades de vigilância, ainda que seja proeminente também sua relação com o circuito de criptomoedas.

ANEXO

CRIPTO-GLOSSÁRIO, Timothy C. May e Eric Hughes (1992)

De: tcmay@netcom.com (Timothy C. May)

Assunto: Cripto Glossário

Data: Sun, 22 Nov 92 11:50:55 PST

Aqui está o glossário de termos de criptografia que divulgamos em formato impresso na primeira reunião da Cypherpunks em Setembro de 1992. Algumas concessões tiveram que ser feitas indo do impresso para o ASCII dessa transmissão, então espero que você tenha paciência comigo.

Estou enviando para a lista inteira porque quase todo mundo que ouve sobre isso diz: "Está online?" e quer uma cópia. Se você não quiser, descarte-o.

Eu não vou manter o "Cypherpunks FAQ", então não me envie correções ou sugestões.

Apreciem!

Tim May

Glossário

(Estas seções introduzirão os termos no contexto, embora as definições completas não sejam dadas)

Adulteração ou escutas telefônicas ativas: interferindo nas mensagens e possivelmente modificando-as. Isso pode comprometer a segurança dos dados, ajudar a quebrar códigos, etc. Veja também *spoofing*.

Agência de Segurança Nacional (NSA): a maior agência de inteligência, responsável por fazer e quebrar cifras, por interceptar comunicações e por garantir a segurança dos computadores dos EUA. Sediada em Fort Meade, Maryland, com muitos postos de escuta em todo o mundo. A NSA financia pesquisa criptográfica e aconselha outras agências sobre questões criptográficas. A NSA, uma vez, obviamente, teve criptógrafos líderes do mundo, mas isso pode não ser mais o caso.

Alice e Bob: protocolos criptográficos são frequentemente explicados considerando-se as partes A e B, ou Alice e Bob, realizando algum protocolo. Eva, a bisbilhoteira, Paulo, o provador, e Victor, o verificador, são outros nomes comuns.

Análise de tráfego: determinar quem está enviando ou recebendo mensagens analisando pacotes, frequência de pacotes, etc. Uma parte da esteganografia (ver Glossário mais adiante). Geralmente tratado com *paping* de tráfego.

ANDOS: tudo ou nada – divulgação de segredos.

Assinatura digital: Analogamente a uma assinatura escrita em um documento. Uma modificação em uma mensagem que somente o assinante pode fazer, mas que todos podem reconhecer. Pode ser usado legalmente para contratar à distância.

Assinaturas e Autenticação: Prova quem você é. Prova que você assinou um documento (e não outra pessoa).

Ataque de texto plano conhecido (*Known-plaintext attack*): uma criptoanálise de uma cifra onde os pares de texto simples e cifrado são conhecidos. Este ataque procura por uma chave desconhecida. Contraste com o ataque de texto plano escolhido, onde o criptoanalista também pode escolher o texto simples a ser cifrado.

Ataque de texto plano escolhido (*Chosen plaintext attack*): um ataque em que o criptoanalista escolhe o texto simples a ser cifrado, por exemplo, quando a posse de uma máquina ou algoritmo de cifra está na posse do criptoanalista.

Autenticação: processo de verificação de uma identidade ou credencial, para garantir que você é quem você disse que era.

***Blinding, blinded signatures* (assinaturas cegas e blindadas)**: Uma assinatura que o assinante não se lembra de ter feito. Uma assinatura cega é sempre um protocolo cooperativo e o receptor da assinatura fornece ao signatário a informação de disfarce.

Blob: o equivalente criptográfico de uma caixa trancada. Um primitivo criptográfico para o comprometimento de bit, com as propriedades que os blobs podem representar um 0 ou um 1, que os outros não podem dizer estar procurando um 0 ou um 1, que o criador do blob pode "abrir" o blob para revelar o conteúdo, e que nenhum blob pode ser um 1 e um 0. Um exemplo disso é uma moeda virada coberta por uma mão.

Canal: o caminho pelo qual as mensagens são transmitidas. Os canais podem ser seguros ou inseguros, e podem ter bisbilhoteiros (ou inimigos, ou disruptores, etc.) que alteram mensagens, inserem e apagam mensagens, etc. Criptografia é o meio pelo qual as comunicações através de canais inseguros são protegidos.

Cartões inteligentes (*Smart cards*): um chip de computador embelezado no cartão de crédito. Eles podem guardar dinheiro, credenciais, chaves criptográficas, etc. Geralmente, eles são construídos com algum grau de resistência à adulteração. Os cartões inteligentes podem executar parte de uma transação criptográfica ou até mesmo completa. Executar parte disso pode significar verificar os cálculos de um computador mais potente, por exemplo, um caixa eletrônico.

Chave pública: a chave distribuída publicamente para potenciais remetentes de mensagens. Pode ser publicado em um diretório semelhante a uma lista telefônica ou enviado de outra forma. Uma das principais preocupações é a validade dessa chave pública para evitar a falsificação.

Chave: uma informação necessária para cifrar ou decifrar uma mensagem. As chaves podem ser roubadas, compradas, perdidas, etc., assim como chaves físicas.

Ciberespaço: o domínio eletrônico, a Internet e os espaços gerados por computador. Alguns dizem que é a "realidade consensual" descrita em "Neuromancer". Outros dizem que é o sistema telefônico. Outros têm trabalho a fazer.

Cifra: uma forma secreta de escrita, usando substituição ou transposição de caracteres ou símbolos.

Cifra assimétrica: mesma coisa que criptografia de chave pública.

Cifra simétrica: o mesmo que o criptosistema de chave privada.

Código: um sistema criptográfico restrito onde palavras ou letras de uma mensagem são substituídas por outras palavras escolhidas de um livro de códigos. Não faz parte da criptologia moderna, mas ainda é útil.

Comprometimento de bit (*Bit commitment*): por exemplo, jogando uma moeda e, em seguida, comprometendo-se com o valor sem ser capaz de mudar o resultado. O blob é uma primitiva criptográfica para isso.

Computacionalmente seguro: onde uma cifra não pode ser quebrada com os recursos de computação disponíveis, mas em teoria pode ser quebrada com recursos de computação suficientes. Contraste com incondicionalmente seguro.

Conluio: em que vários participantes cooperam para deduzir a identidade de um remetente ou destinatário, ou para quebrar uma cifra. A maioria dos sistemas criptográficos é sensível a algumas formas de conluio. Grande parte do trabalho na implementação de redes de controle de tráfego, por exemplo, envolve a garantia de que os coletores não podem isolar os remetentes de mensagens e, portanto, rastrear origens e destinos de correspondência.

Contramedida: algo que você faz para impedir um invasor.

Credencial: fatos ou afirmações sobre alguma entidade. Por exemplo, classificações de crédito, passaportes, reputações, status fiscal, registros de seguro, etc. No sistema atual, essas credenciais estão sendo cada vez mais interligadas. Assinaturas cegas podem ser usadas para criar credenciais anônimas.

Credencial anônima: uma credencial que afirma algum direito, privilégio ou fato sem revelar a identidade do titular. Isso é diferente das licenças de dirigir da Califórnia.

Credencial clearinghouse: bancos, agências de crédito, companhias de seguro, departamentos de polícia, etc., que correlacionam registros e decidem o status dos registros.

Credencial negativa: uma credencial que você possui e que não quer que ninguém mais saiba, por exemplo, um pedido de falência. Uma versão formal de uma reputação negativa.

Criptoanálise Diferencial de Shamir-Biham: técnica para criptoanálise do DES (ver mais adiante nesse glossário). Com um ataque de texto plano escolhido (*chosen plaintext attack*), eles reduziram o número de chaves DES que devem ser testadas de cerca de 2^56 para cerca de 2^47 ou menos. Observe, no entanto, que raramente um invasor pode montar um ataque de texto plano escolhido em sistemas DES.

Criptoanálise: métodos para atacar e quebrar cifras e sistemas criptográficos relacionados. As cifras podem ser quebradas, o tráfego pode ser analisado e as senhas podem ser quebradas. Computadores são naturalmente essenciais.

Criptoanarquia: sistema econômico e político após a implantação de criptografia, e-mails não rastreáveis, pseudônimos digitais, votação criptográfica e dinheiro digital. Um trocadilho com "criptografia", que significa "hipem", e como quando Gore Vidal chamou William F. Buckley de "criptista fascista". Uma solução lógica para o problema do excesso de governo.

Criptografia: Privacidade de mensagens usando cifras e códigos para proteger o sigilo de mensagens. DES é a cifra simétrica mais comum (mesma chave para cifragem e decifragem). RSA é a cifra assimétrica mais comum (chaves diferentes para cifrar e decifrar).

Criptografia de chave pública: o uso de métodos criptográficos modernos para fornecer segurança e autenticação de mensagens. O algoritmo RSA é a forma mais amplamente usada de criptografia de chave pública, embora existam outros sistemas. Uma chave pública pode ser livremente publicada, por exemplo, em diretórios semelhantes à agenda telefônica, enquanto a chave privada correspondente é protegida de perto.

Criptografia probabilística: um esquema de Goldwasser, Micali e Blum que permite múltiplos textos cifrados para o mesmo texto simples, isto é, qualquer texto plano dado pode ter muitos textos cifrados se a cifragem for repetida. Isso protege contra certos tipos de ataques de texto cifrado conhecidos no RSA.

Criptografia Quântica: Bisbilhoteiros mudam o estado quântico do sistema e são detectados. Desenvolvido por Brassard e Bennett, apenas pequenas demonstrações laboratoriais foram feitas.

Criptologia: a ciência e o estudo de escrever, enviar, receber e decifrar mensagens secretas. Inclui autenticação, assinaturas digitais, ocultação de mensagens (esteganografia), criptoanálise e vários outros campos.

Criptosistema de chave pública: o avanço moderno em criptologia, projetado por Diffie e Hellman, com contribuições de vários outros. Usa as funções unidirecionais de interceptação para que a cifração possa ser feita por qualquer pessoa com acesso à "chave pública", mas a decifração pode ser feita apenas pelo detentor da "chave privada". Abrange criptografia de chave pública, assinaturas digitais, dinheiro digital e muitos outros protocolos e aplicativos.

Criptosistema de chave secreta: Um sistema que usa a mesma chave para cifrar e decifrar o tráfego em cada extremidade de um link de comunicação. Também chamado de sistema simétrico ou de uma chave. Contraste com o sistema criptográfico de chave pública.

***Cyphertext* (texto cifrado)**: o texto, é claro, depois de ter sido cifrado.

DES: "Data Encryption Standard" ou Padrão de Criptografia de Dados, proposto em 1977 pelo National Bureau of Standards (agora NIST), com assistência da National Security Agency (NSA). Com base na cifra "Lucifer" desenvolvida por Horst Feistel na IBM, o DES é um sistema criptográfico de chave secreta com ciclos e blocos de dados de 64 bits por meio de várias permutações com uma chave de 56 bits controlando o roteamento. "Difusão" e "confusão" são combinados para formar uma cifra que ainda não sofreu criptoanálise (veja "DES, Segurança de"). O DES está em uso para transferências interbancárias, como uma codificação dentro de vários sistemas baseados em RSA, e está disponível para PCs.

DES, Segurança de: muitos especularam que a NSA colocou um backdoor (ou porta dos fundos) no DES para permitir a leitura de mensagens criptografadas no DES. Isso não foi provado. Sabe-se que o algoritmo original de Lucifer usou uma chave de 128 bits e que esse comprimento de chave foi reduzido para 64 bits (56 bits mais 8 bits de paridade), tornando a busca exaustiva muito mais fácil (até onde se sabe, busca por força bruta não foi feito, embora deva ser viável hoje). Shamir e Bihan usaram uma técnica chamada "criptoanálise diferencial" para reduzir a busca exaustiva necessária para ataques de texto puro escolhidos (mas sem importar para DES ordinários).

Descrição: Seja ***p*** e ***q*** grandes primos com mais de 100 dígitos. Seja n = pq e encontre algum **e** tal que **e** seja relativamente primo para (p − 1) (q − 1). O conjunto de números **p**, **q** e **e** é a chave privada do RSA. O conjunto de números ***n*** e ***e*** formam a chave pública (lembre-se de saber **n** não é suficiente para facilmente encontrar **p** e **q** ... o problema de fatoração). Uma mensagem M é cifrada através do cálculo do **M^*e*** mod n**.** O proprietário da chave privada pode decifrar a mensagem cifrada explorando os resultados da teoria dos números, da seguinte maneira. Um inteiro ***d*** é computado de modo que **ed = 1 (mod (p − 1) (q − 1))**. Euler provou um teorema que **M ^(ed) = M mod n** e assim **M ^ (ed) mod n = M**. Isto significa que

em certo sentido os inteiros ***e*** e ***d*** são "inversos" um do outro. [Se isso não estiver claro, consulte um dos muitos textos e artigos sobre criptografia de chave pública].

Digital timestamping: uma função de um notário digital, em que alguma mensagem (uma música, roteiro, caderno de laboratório, contrato, etc.) é carimbada com um tempo que não pode (facilmente) ser falsificado.

Dinheiro Digital: Foco: privacidade em transações, compras, credenciais não vinculáveis, notas blindadas. "Moedas digitais" podem não ser possíveis.

DSS, Padrão de Assinatura Digital: o mais recente padrão do NIST (Instituto Nacional de Padrões e Tecnologia, sucessor do NBS) para assinaturas digitais. Com base na cifra de El Gamal, alguns consideram o substituto fraco e pobre para esquemas de assinatura baseados em RSA.

Email não rastreável: um sistema para enviar e receber correio sem rastreabilidade ou observabilidade. Receber correio anonimamente pode ser feito com a transmissão do correio de forma criptografada. Somente o destinatário pretendido (cuja identidade, ou nome verdadeiro, pode ser desconhecido do remetente) pode decifrar a mensagem. Enviar correio anonimamente aparentemente requer misturas ou uso do protocolo de criptógrafos de restaurantes. Foco: derrotar os bisbilhoteiros e análise de tráfego. Uso do protocolo DC (*dining cryptographers*).

Escutas (eavesdropping), ou escutas telefônicas passivas: interceptando mensagens sem detecção. As ondas de rádio podem ser interceptadas, as linhas telefônicas podem ser tocadas e os computadores podem ter emissões de RF detectadas. Até mesmo linhas de fibra óptica podem ser aproveitadas.

Esteganografia: uma parte da criptologia que lida com esconder mensagens e obscurecer quem está enviando e recebendo mensagens. Muitas vezes, o tráfego de mensagens é enviado para reduzir os sinais que,

de outra forma, viriam de um começo suspenso de mensagens. Também um ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido. Enquanto a criptografia oculta o significado da mensagem, a esteganografia oculta a existência da mensagem.

Exponenciação modular: elevando um inteiro para o expoente de outro inteiro, modulo algum inteiro. Para inteiros a, n e m, a^m mod n. Por exemplo, 5^3 mod 100 = 25. A exponenciação modular pode ser feita rapidamente com uma sequência de deslocamentos de bit e aps, e chips de propósito especial foram projetados. Veja também logaritmo discreto.

Fatoração: Alguns números grandes são difíceis de fatorar. É conjecturado que não existem métodos factíveis – isto é, "fáceis", menos exponenciais em tamanho de número – de factoring. Também é um problema aberto se o RSA pode ser quebrado mais facilmente do que fatorando o módulo (por exemplo, a chave pública pode revelar informações que simplificam o problema). Curiosamente, embora se acredite que a fatoração seja "difícil", não se sabe que se trata da classe dos problemas difíceis do NP-difícil. O professor Janek inventou um dispositivo de fatoração, mas acredita-se que ele seja fictício.

Função de via única (*One-way function*): uma função que é fácil calcular em uma direção, mas difícil de computar na direção inversa; por exemplo, exponenciação modular, onde o problema inverso é conhecido como o problema do logaritmo discreto. Compare o caso especial de funções unidirecionais de *trapdoor*. Um exemplo de operação unidirecional é a multiplicação: é fácil multiplicar dois números primos de 100 dígitos para produzir um número de 200 dígitos, mas é difícil fatorar esse número de 200 dígitos.

Funções de sentido único de trap-door (*Trap-door one way functions*): funções que são fáceis de calcular tanto na direção para frente quanto na reversa, mas para as quais a revelação de um algoritmo para computar a função na direção certa não fornece informações sobre como calcular a função na direção reversa.

Mais simplesmente, as funções de um lado do *trap-door* são um caminho para todos menos o detentor da informação secreta. O algoritmo RSA é o exemplo mais conhecido de tal função.

Incondicionalmente seguro: onde nenhuma quantidade de texto cifrado interceptado é suficiente para permitir que a cifra seja quebrada, como com o uso de uma cifra de uso único (one time pad). Contraste com computacionalmente seguro.

Lançamento de moeda: uma importante primitiva criptográfica, ou protocolo, no qual o equivalente de lançar uma moeda justa é possível. Implementado com blobs.

Mensagens de armadilha (*Trap messages*): Mensagens fictícias em Redes DC que são usadas para capturar jammers e disruptores. As mensagens não contêm informações particulares e são publicadas em um *blob* antecipadamente, de modo que a mensagem de interceptação possa mais tarde ser aberta para revelar o disruptor. (Existem muitas estratégias para explorar aqui).

***Misturadores* (Mixes)**: O termo de David Chaum para uma caixa que desempenha a função de misturar ou descorrelacionar mensagens de correio eletrônico recebidas e enviadas. A caixa também retira o envelope externo (ou seja, descriptografa com sua chave privada) e repassa a mensagem para o destinatário no envelope interno. Módulos resistentes a violações podem ser usados para evitar fraudes e divulgação forçada do mapeamento entre mensagens recebidas e enviadas. Uma sequência de muitos reencaminhamentos faz com que o envio e o recebimento do rastreio sejam impossíveis. Compare isso com a versão do software, o protocolo DC.

Módulos de resposta a violações, módulos resistentes a violações (TRMs): caixas seladas ou módulos que são difíceis de abrir, exigindo extensa sondagem e geralmente deixando ampla evidência de que a adulteração ocorreu. Várias técnicas de proteção são usadas, como camadas especiais de metal ou óxido em chips, revestimentos blindados, fibras óticas embainhadas e outras medidas para impedir a análise. Popularmente chamado de "caixas invioláveis". Os usos incluem: cartões inteligentes, iniciadores de armas nucleares, detentores de chaves criptográficas, caixas eletrônicos etc.

Moeda digital, dinheiro digital: Protocolos para transferência de valor, monetário ou eletronicamente. Dinheiro digital geralmente se refere a sistemas que são anônimos. Sistemas monetários digitais podem ser usados para implementar qualquer quantidade que seja conservada, como pontos, massa, dólares, etc. Existem muitas variações dos sistemas de dinheiro digital, variando de números VISA a moedas digitais assinadas às cegas. Um tópico muito grande para uma única entrada de glossário.

NP-completo: uma grande classe de problemas difíceis. "NP" significa tempo polinomial não determinístico, uma classe de problemas que, em geral, não possuem algoritmos viáveis para sua solução. Um problema é "completo" se qualquer outro problema de NP puder ser reduzido a esse problema. Muitos problemas combinatórios e algébricos importantes são NP-completos: o problema do vendedor ambulante, o problema do ciclo hamiltoniano, o problema da palavra e assim por diante.

Números Primos: inteiros sem nenhum outro fator além deles mesmos e 1. O número de primos são ilimitados. Cerca de 1% dos 100 números de dígitos decimais são primos. Como existem cerca de 10^70 partículas no universo, existem cerca de 10^23 números primos de 100 dígitos para cada uma das partículas do universo!

***One-time pad* (OTP)**: uma sequência de bits ou símbolos selecionados aleatoriamente que é combinada com uma mensagem de texto simples para produzir o texto cifrado. Essa combinação pode estar alterando algumas letras, bit-a-bit com ou-exclusivo, etc. O destinatário, que também possui uma cópia do *one time pad*, pode recuperar facilmente o texto simples. Desde que o pad seja usado apenas uma vez e depois destruído, e não esteja disponível para um interceptador, o sistema é perfeitamente seguro, ou seja, é teoricamente seguro. A distribuição de chaves (o bloco) é obviamente uma preocupação prática, mas considere os CD-ROMs.

P ?=? NP: Certamente o mais importante problema não resolvido na teoria da complexidade. Se **P = NP**, então a criptografia como a conhecemos hoje não existe. Se **P = NP**, todos os problemas de NP são "fáceis".

Papeando (*Paping*): enviar mensagens extras para confundir bisbilhoteiros e para derrotar a análise de tráfego. Também imitando bits aleatórios a uma mensagem a ser codificada.

Patentes de chave pública: M.I.T. e Stanford, devido ao trabalho de Rivest, Shamir, Adleman, Diffie, Hellman e Merkle, formou Public Key Partners para licenciar as várias patentes públicas, assinaturas digitais e patentes da RSA. Essas patentes, concedidas no início dos anos 80, expiram entre 1998 e 2002. A PKP licenciou a RSA Data Security Inc., de Redwood City, CA, que administra as vendas, etc.

***Plaintext* (Texto plano)**: também chamado de texto claro, o texto a ser cifrado.

***Pretty Good Privacy* (PGP)**: A implementação do RSA feita por Phillip Zimmerman, recentemente atualizada para a versão 2.0, com componentes mais robustos e vários novos recursos. A RSA Data Security ameaçou o PZ, portanto ele não trabalha mais nela. A versão 2.0 foi escrita por um consórcio de hackers de fora dos EUA.

Problema do logaritmo discreto: dados inteiros **a**, **n** e **x**, encontre algum inteiro **m** tal que **a^m mod n = x**, se **m** existir. A exponenciação modular, a^m mod n, a parte mais moderna, é simples de executar (e chips para fins especiais estão disponíveis), mas acredita-se que o problema inverso seja muito difícil, em geral. Assim, conjectura-se que a exponenciação modular é uma função unidirecional.

Protocolo DC ou DC-Net: O protocolo jantar dos criptógrafos (*dining cryptographers*). As DC-Nets usam múltiplos participantes se comunicando com o protocolo DC.

Protocolo dos criptógrafos de jantar (aka *DC protocol, DC nets*): o sistema de envio de mensagens não rastreável inventado por David Chaum. Nomeado após o problema dos "filósofos de jantar" na ciência da computação. Os participantes formam circuitos e passam mensagens de tal maneira que a origem não pode ser deduzida, exceto o conluio. No nível mais simples, dois participantes compartilham uma chave entre eles. Um deles envia alguma mensagem real bit-a-bit

com ou-exclusivo (XOR) entre a mensagem e a chave, enquanto o outro apenas envia a chave em si. A mensagem real deste par de participantes é obtida pela XOR das duas saídas. No entanto, como ninguém além do par conhece a chave original, a mensagem real não pode ser atribuída a nenhum dos participantes.

Protocolo: um procedimento formal para resolver algum problema. A Criptologia moderna é principalmente sobre o estudo de protocolos para muitos problemas, tais como "jogar moedas", *bit commitment* (blobs), provas de conhecimento zero, criptógrafos de jantar e assim por diante.

Provas de conhecimento zero (*Zero knowledge proofs*): provas em que nenhum conhecimento da prova real é transmitido. Ex: Peggy, o Provador, demonstra a Sid, o Cético, que ela está realmente de posse de algum conhecimento sem realmente revelar nada desse conhecimento. Isso é útil para o acesso a computadores, porque bisbilhoteiros ou *sysops* desonestos não podem roubar o conhecimento dado. Também chamado de provas mínimas de divulgação. Útil para provar a posse de alguma propriedade ou credencial, como idade ou status de votação, sem revelar informações pessoais.

Provas de identidade: provando quem você é, seu nome verdadeiro ou sua identidade digital. Geralmente, a posse da chave certa é prova suficiente (proteja sua chave!). Algum trabalho foi feito em agências de credenciamento "é uma pessoa", usando o chamado protocolo Fiat-Shamir... pense nisso como uma maneira de emitir passaportes digitais não passíveis de assinatura. A prova física de identidade pode ser feita com métodos de segurança biométrica. Provas de identidade zero conhecimento não revelam nada além do fato de que a identidade é como reivindicada. Isso tem usos óbvios para acesso a computadores, senhas etc.

Provas mínimas de divulgação (*Minimum disclosure proofs*): outro nome para provas de conhecimento zero, favorecido por Chaum.

Pseudônimo digital: basicamente, uma "identidade cripto". Uma maneira de os indivíduos configurarem contas com várias organizações sem revelar mais informações do que desejam. Os usuários podem

ter vários pseudônimos digitais, alguns usados apenas uma vez, alguns usados ao longo de muitos anos. Idealmente, os pseudônimos podem ser vinculados somente à vontade do portador. Na forma mais simples, uma chave pública pode servir como um pseudônimo digital e não precisa estar vinculada a uma identidade física.

Regras de transmissão: os protocolos para determinar quem pode enviar mensagens em um protocolo DC e quando. Essas regras são necessárias para evitar a colisão e o bloqueio deliberado dos canais.

Reputações: o rastro de associações positivas e negativas e julgamentos que algumas entidades acumulam. Classificações de crédito, credenciais acadêmicas e confiabilidade são exemplos. Um pseudônimo digital acumulará essas credenciais de reputação com base em ações, opiniões de outros, etc. Na criptoanarquia, reputações e sistemas agoristas serão de suma importância. Há muitas questões fascinantes sobre como os sistemas baseados em reputação funcionam, como as credenciais podem ser compradas e vendidas e assim por diante.

RSA: o principal algoritmo de criptografia de chave pública, desenvolvido por Ron Rivest, Adi Shamir e Kenneth Adleman. Ele explora a dificuldade de fatorar números grandes para criar uma chave privada e uma chave pública. Inventado pela primeira vez em 1978, ele continua sendo o núcleo dos modernos sistemas de chaves públicas. Geralmente é muito mais lento que o DES, mas os chips de exponenciação modular de propósito especial provavelmente vão acelerar. Um esquema popular de velocidade é usar o RSA para transmitir chaves de sessão e, em seguida, uma codificação de alta velocidade, como DES, para o texto da mensagem real.

Segurança biométrica: um tipo de autenticação usando impressões digitais, exames de retina, impressões palmares ou outras assinaturas físicas / biológicas de um indivíduo.

Segurança incondicional: o mesmo que a sigilo perfeito da teoria da informação, isto é, inquebrável, exceto pela perda ou roubo da chave.

Segurança teórica da informação "inquebrável": segurança, na qual nenhuma quantidade de criptoanálise pode quebrar uma cifra ou sistema. *One Time Pad* são um exemplo (desde que os pads não sejam perdidos nem roubados nem usados mais de uma vez, é claro). O mesmo que incondicionalmente seguro.

Sistemas agoristas: sistemas abertos de livre mercado nos quais as transações voluntárias são centrais.

***Spoofing* (enganar), ou *masquerading* (mascarar)**: posando como outro usuário. Usado para roubar senhas, modificar arquivos e roubar dinheiro. Assinaturas digitais e outros métodos de autenticação são úteis para evitar isso. As chaves públicas devem ser validadas e protegidas para garantir que outras pessoas não substituam suas próprias chaves públicas, que os usuários podem usar inadvertidamente.

Token: alguma representação, como cartões de identificação, fichas de metrô, dinheiro, etc., que indica a posse de alguma propriedade ou valor.

Transferência inconsciente *(oblivious transfer)*: uma primitiva criptográfica que envolve a transmissão probabilística de bits. O remetente não sabe se os bits foram recebidos.

Trap-door: Na criptografia, uma informação secreta que permite ao detentor de uma chave privada inverter uma função normalmente difícil de inverter.

Troca de chaves ou distribuição de chaves: o processo de compartilhar uma chave com alguma outra parte, no caso de cifras simétricas, ou de distribuir uma chave pública em uma cifra assimétrica. Uma questão importante é que as chaves sejam trocadas de forma confiável e sem compromisso. Diffie e Hellman criaram um desses esquemas, baseado no problema do logaritmo discreto.

Voto criptográfico: Vários esquemas foram criados para votação anônima e não rastreável. Os esquemas de votação devem ter várias propriedades: privacidade do voto, segurança do voto (sem votos múltiplos), robustez contra interrupções por bloqueadores ou bloqueadores, verificabilidade (o eleitor confia nos resultados) e eficiência. Foco: anonimato na urna, credenciais para votar, questões de dupla votação, segurança, robustez, eficiência.


THIS MACHINE KILLS FASCISTS

A coleção Tecnopolítica busca trazer textos considerados clássicos e outros inéditos sobre a vasta discussão em torno da tecnologia e suas relações com a sociedade, a cultura e a comunicação. Quer fazer circular artigos, ensaios e manifestos que pensaram - ou estão pensando hoje - os impactos da internet e do digital no dia a dia das pessoas.

Os Manifestos Cypherpunks são alguns dos primeiros alertas contra a vigilância massiva na era da internet. Foram escritos entre o final dos anos 1980 até meados dos 1990 por pessoas que conheciam a fundo os aparatos técnicos que faziam funcionar a rede e queriam nos fazer ficar atentos a eles. Uma vez que uma infraestrutura de comunicações otimizada para a vigilância se torna arraigada, uma mudança nas condições políticas podem levar ao abuso desse poder recém-descoberto.

ISBN 978-65-86008-17-3