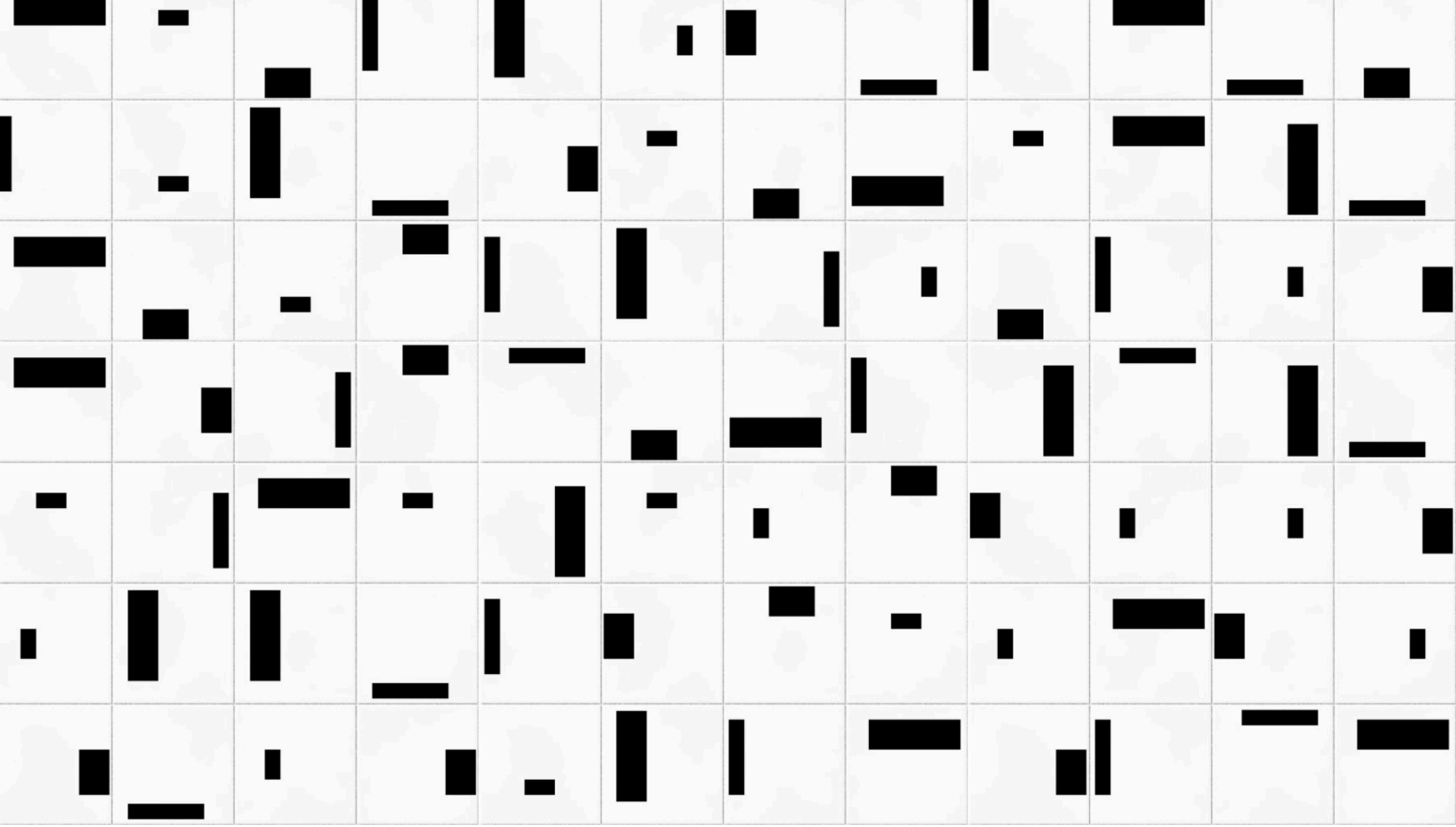


paniel de alexandre mancini

A RELAÇÃO DO BRASIL COM A CRIPTOGRAFIA

JACQUELINE ABREU

INTERNETLAB

24/08/2016

APRESENTAÇÃO

- internetlab
- centro de pesquisa em direito e tecnologia
- **vigilância e privacidade**
- *criptografia*: privacidade e segurança ou privacidade x segurança?
- **relação do Brasil com a criptografia**

PANO DE FUNDO

> bloqueios do WhatsApp

> proposta de regulamentação?

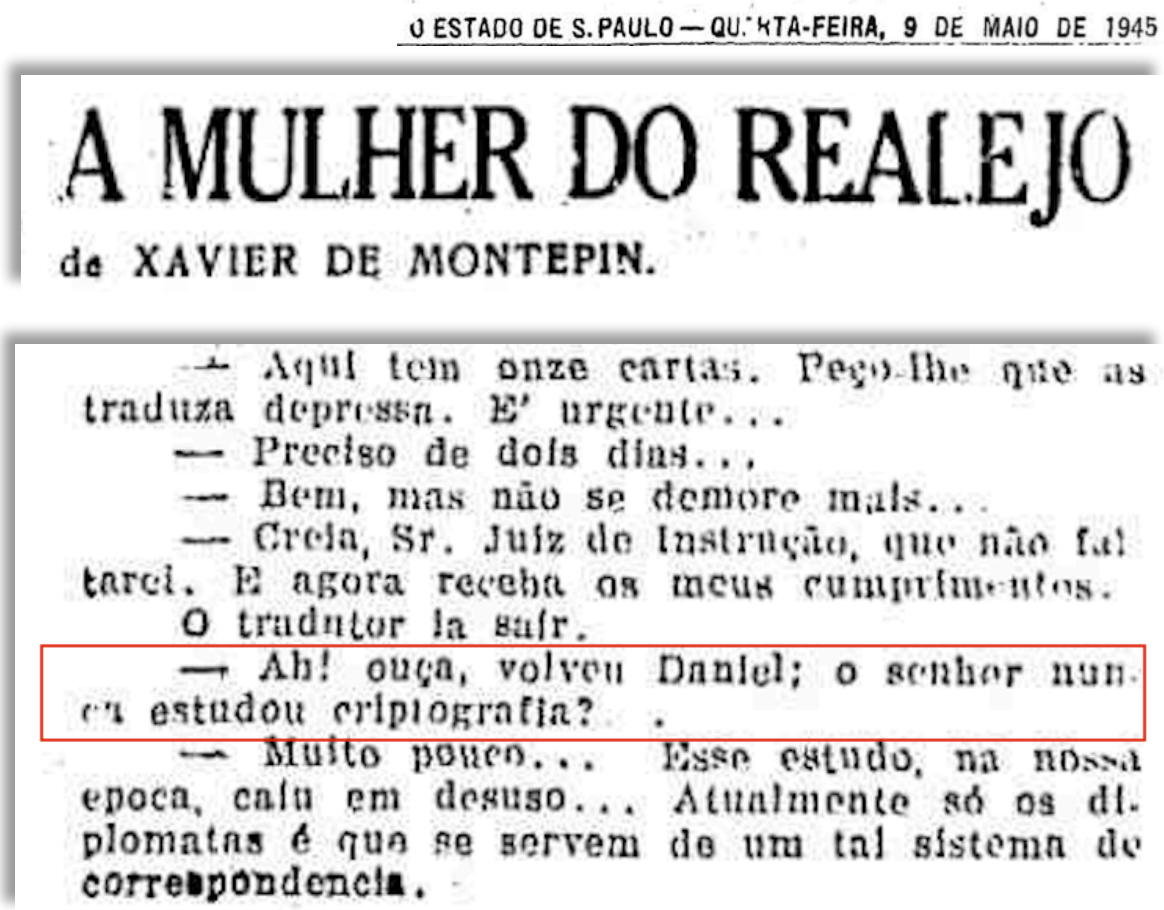
> internacional: Apple v. FBI; ameaças terroristas; criptografia culpada?

Como chegamos a este ponto?

Para onde devemos ir?

IRONIA HISTÓRICA

quando primeiro se falou em cripto em jornal



O ESTADO DE S. PAULO — QUARTA-FEIRA, 9 DE MAIO DE 1945

A MULHER DO REALEJO

de XAVIER DE MONTEPIN.

— Aqui tem onze cartas. Peço-lhe que as traduza depressa. E' urgente...

— Preciso de dois dias...

— Bem, mas não se demore mais...

— Creia, Sr. Juiz de Instrução, que não faltarei. E agora receba os meus cumprimentos.

O tradutor ia saír.

— Ah! ouça, volveu Daniel; o senhor nunca estudou criptografia?

— Muito pouco... Esse estudo, na nossa epoca, caiu em desuso... Atualmente só os diplomatas é que se servem de um tal sistema de correspondencia.

ORIGENS DE UMA TENSÃO

Estados e criptografia: uma relação ambivalente

- Serviços Secretos
- CRIPTOGRAFIA é
  - excelente para "proteção" de informações do Estado
  - péssima para "produção" de informações sobre outros Estados e indivíduos

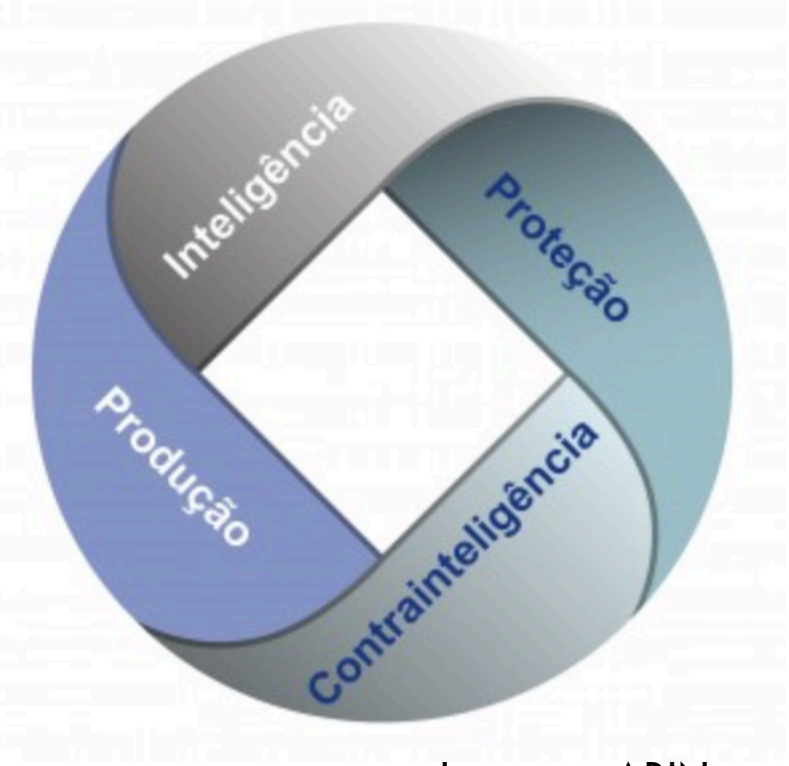


Imagem: ABIN

BRASIL S2 CRIPTOGRAFIA I

Brasil abandona padrão de criptografia maculado pela NSA

Luís Osvaldo Grossmann ... 27/05/2014 ... Convergência Digital

Sem nenhum alarde, o governo brasileiro descartou, há cerca de três meses, um dos padrões criptográficos dos certificados digitais do sistema de chaves públicas ICP Brasil. Trata-se da versão 3, ou simplesmente V3, da cadeia de certificação – o que seria o namoro do sistema nacional de certificação digital com a criptografia por curvas elípticas.

Formalmente, alegou-se que não houve adesão das autoridades certificadoras. E, efetivamente, não há certificados emitidos com a V3. A decisão de revogar essa linha de certificados, no entanto, é a primeira resposta concreta às denúncias da espionagem indiscriminada dos Estados Unidos – e, especialmente, do envolvimento da NSA na

BRASIL S2 CRIPTOGRAFIA II

ESTADÃO

Abin cria sistemas de criptografia para proteger dados do governo

Lisandra Paraguassu, O Estado de S. Paulo

07 Setembro 2013 | 19h01

Feitos para proteger dados de espiões e sistemas de monitoramento, o CriptoGOV e o cGOV devem estar prontos para uso nos próximos dias. Os novos equipamentos foram apresentados no Planalto em 14

Brasil emprega criptografia quando é para proteger a **privacidade de suas próprias comunicações** e a **segurança do estado.**

Já quando se trata da **privacidade** e **segurança de dados dos cidadãos...**

CRIPTO CHEGA AO PÚBLICO

O ESTADO DE S. PAULO — 25

QUARTA-FEIRA — 5 DE JULHO DE 1978

Atualidade Científica

Nova técnica contra ouvintes clandestinos

Violadores de códigos e ouvintes clandestinos de aparelhos eletrônicos vão deixar de ser uma preocupação, graças a um achado em criptografia desenvolvido por três engenheiros eletricistas da Universidade Stanford, na Califórnia

O professor Martin E Hel

problema de distr
chaves

"Um sistema c
lhão de usuários ex
madamente 500 0
de chaves diferente
ra cada par em p
interlocutores"
professor Hellman
pode enviá-las pe

CRIPTO CHEGA AO PÚBLICO

WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 07.31.16 6:45 AM

MEET MOXIE MARLINSPIKE, THE ANARCHIST BRINGING ENCRYPTION TO ALL OF US

CRIPTOGRAFIA PARA CIDADÃOS

FAZENDO O QUE FOI CRIADA PARA FAZER

> garante confidencialidade e segurança de dados contra terceiros mal-intencionados e bisbilhoteiros

Imagem: Google Transparency Report

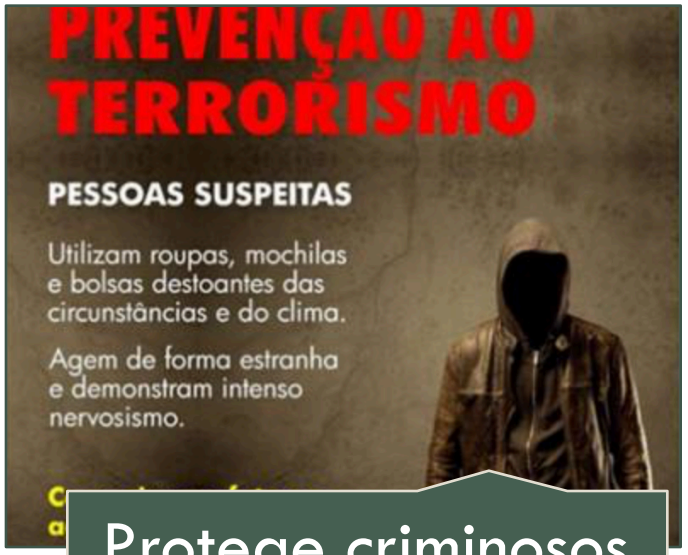
CRIPTOGRAFIA PARA CIDADÃOS

O PAPEL DAS EMPRESAS DE TECNOLOGIA

> problema aparece quando empresas **não mantém uma "chave-mestra"**

CRÍTICAS À CRIPTOGRAFIA

"Going dark"



Protege criminosos e terroristas

"GOING DARK": É ISSO MESMO?

- Não há evidência empírica "macro"
- Há outras formas: "Golden Age of Surveillance"

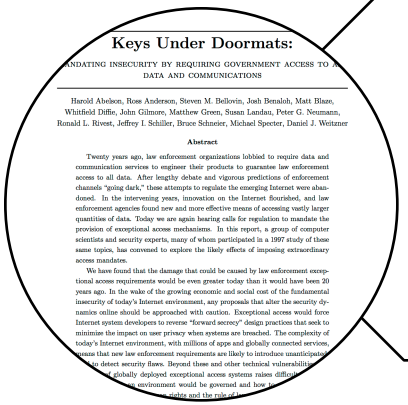
SOLUÇÕES DEFENDIDAS

BACKDOOR? ACESSO PRIVILEGIADO? REGULAMENTAR?

PODER JUDICIÁRIO
DO ESTADO DO RIO DE JANEIRO
2ª VARA CRIMINAL
DA COMARCA DE DUQUE DE CAXIAS

Em verdade, o Juízo requer, apenas, a desabilitação da chave de criptografia, com a interceptação do fluxo de dados, com o desvio em tempo real em uma das formas sugeridas pelo MP, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia.

O QUE DIZEM ESPECIALISTAS



Keys Under Doormats:

MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS

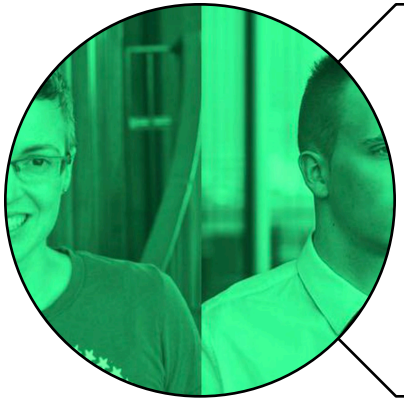
Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Abstract

Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels "going dark," these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today we are again hearing calls for regulation to mandate the provision of exceptional access mechanisms. In this report, a group of computer scientists and security experts, many of whom participated in a 1997 study of these same topics, has convened to explore the likely effects of imposing extraordinary access mandates.

We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse "forward secrecy" design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated ... to detect security flaws. Beyond these and other technical vulnerabilities ... of globally deployed exceptional access systems raises difficult ... environment would be governed and how ... rights and the rule of ...

"The goal of this report is to similarly analyze the newly proposed requirement of exceptional access to communications in today's more complex, global information infrastructure. We find that it would pose far more grave security risks, imperil innovation, and raise thorny issues for human rights and international relations."



"O debate sobre a criptografia versus aplicação da lei é um debate "segurança versus segurança", não um debate "privacidade versus segurança". Se a criptografia é quebrada para a aplicação da lei, esse mesmo *backdoor* poderá ser usado por bandidos também".

CRIPTO "PROTEGE" BANDIDOS?

tec

Criminosos usam iPhone por causa da criptografia, dizem policiais dos EUA

Essa referência ao aplicativo whatsapp, onde criminosos que estão sendo interceptados deixam de falar ao telefone e indicam que preferem se comunicar através do referido aplicativo, são verificadas em diversas investigações, sem que a Justiça nada possa fazer!

PJERJ

- Isso não é novidade; tecnologias podem ser usadas "para o bem" ou "para o mal".

É ISSO MESMO?

REFLEXÕES

- Impossibilidade técnica muda 'default'
- investigar outros fatores:
  - investimento em outras técnicas;
  - MLAT com gargalho.
- efeitos técnicos, econômicos e políticos de regular criptografia

OS DIREITOS AUTORAIS DESSA APRESENTAÇÃO DE PPT

OBRIGADA!

Jacqueline de Souza Abreu

jacqueline@internetlab.org.br

@jacqueabreu

http://www.internetlab.org.br