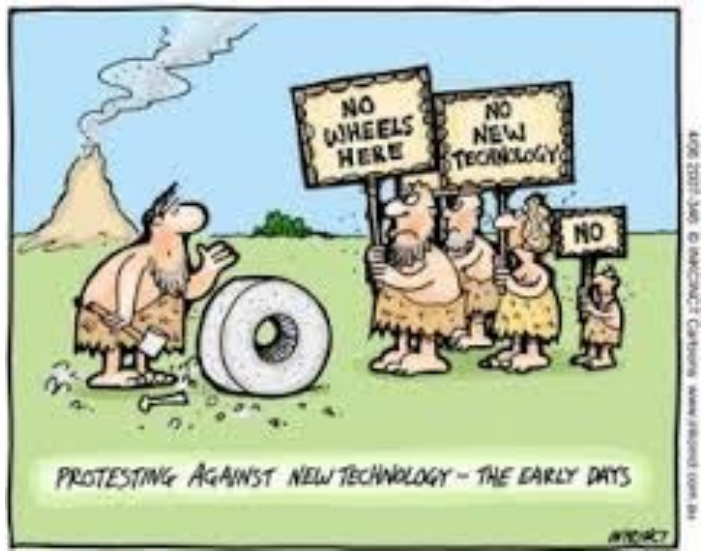
Audiência Pública: A segurança e a transparência do sistema eleitoral brasileiro e a confiabilidade das urnas eletrônicas

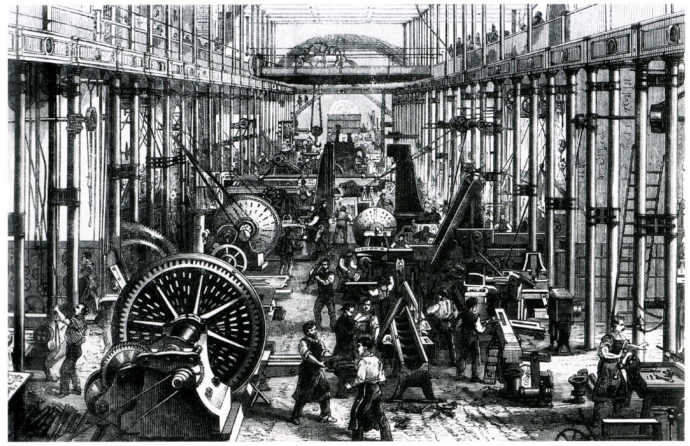
Evolução e segurança

Prof. Avelino F. Zorzo – PUCRS e SBC
avelino.zorzo@pucrs.br

Evolução da sociedade

Evolução da sociedade …





Mundo Físico

(conhecido?)

Física
- Eletricidade
- Aeronáutica
- ....

Química
- Medicamentos
- Combustíveis
- ....

Biologia
- Alimentos
- Corpo humano
- ....

Mundo Digital

(desconhecido)

Internet

Ciência de Dados

Algoritmo

Robôs

Inteligência Artificial

Criptografia

Redes Sociais

Evolução: sistemas de votação

Voto “cantado”

Eleição municipal (Missouri, c.1846) George Caleb Bingham 1851-2

http://homepage.cs.uiowa.edu/~jones/voting/pictures/

Voto “cantado” - Problemas?

Eleição municipal (Missouri, c.1846) George Caleb Bingham 1851-2

http://homepage.cs.uiowa.edu/~jones/voting/pictures/

Privacidade
Voto de cabresto
Pagamento
...

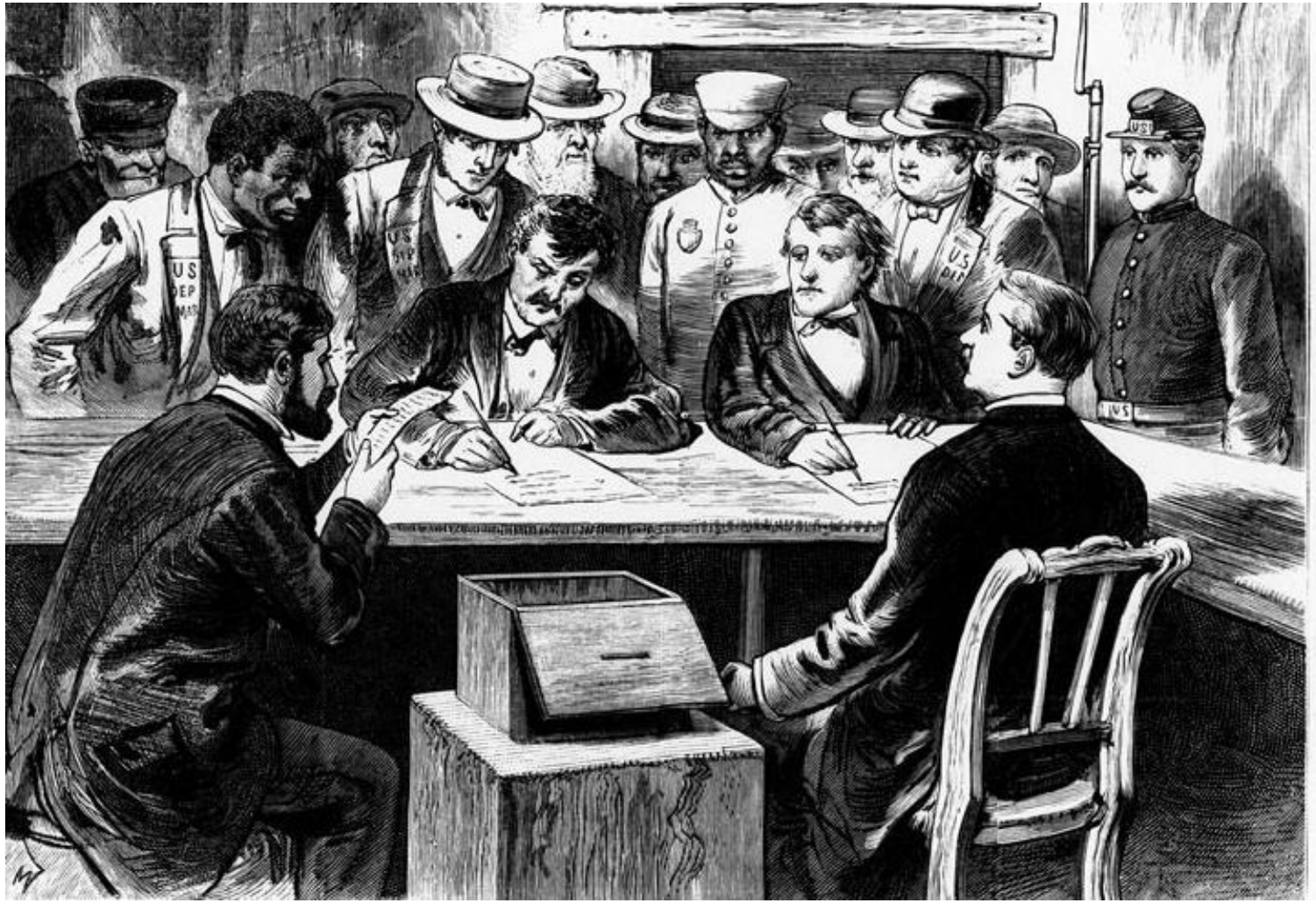
Diferentes tipos de urnas

http://americanhistory.si.edu/vote/patchwork.html

http://americanhistory.si.edu/vote/patchwork.html

http://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/709

Contagem de votos em papel



http://americanhistory.si.edu/vote/paperballots.html

Contagem de votos em papel

https://noticias.uol.com.br/politica/ultimas-noticias/2021/08/06/eleicoes-antes-das-urnas-eletronicas.htm

Apuração das eleições para o governo de São Paulo em 1990
Imagem: Sérgio Amaral/Estadão

Contagem de votos em papel

https://noticias.uol.com.br/politica/ultimas-noticias/2021/08/06/eleicoes-antes-das-urnas-eletronicas.htm

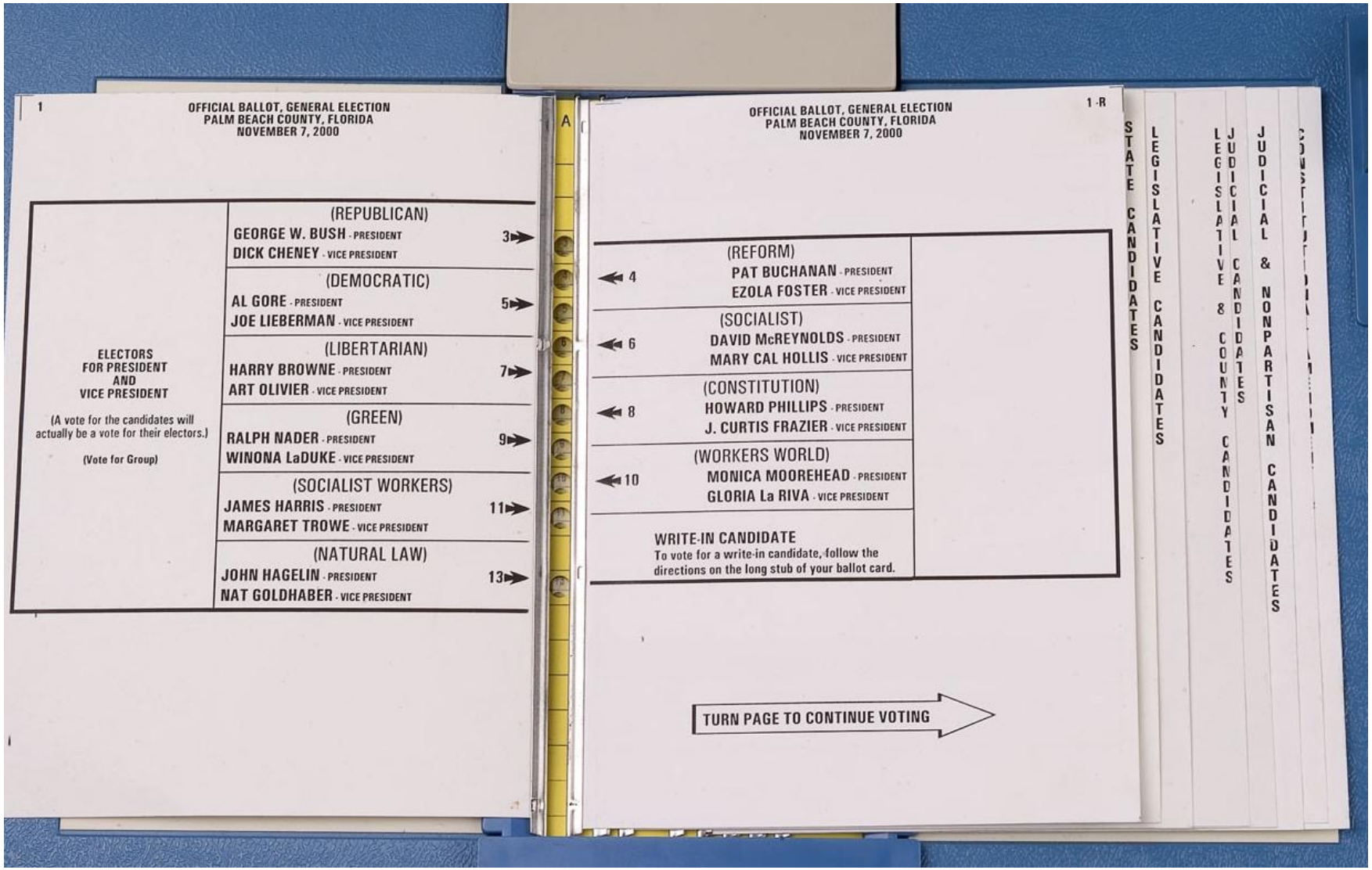
Apuração dos votos do segundo turno para eleições presidenciais em 1989
Imagem: Sérgio Amaral/Estadão

Sistemas mecânicos de votação

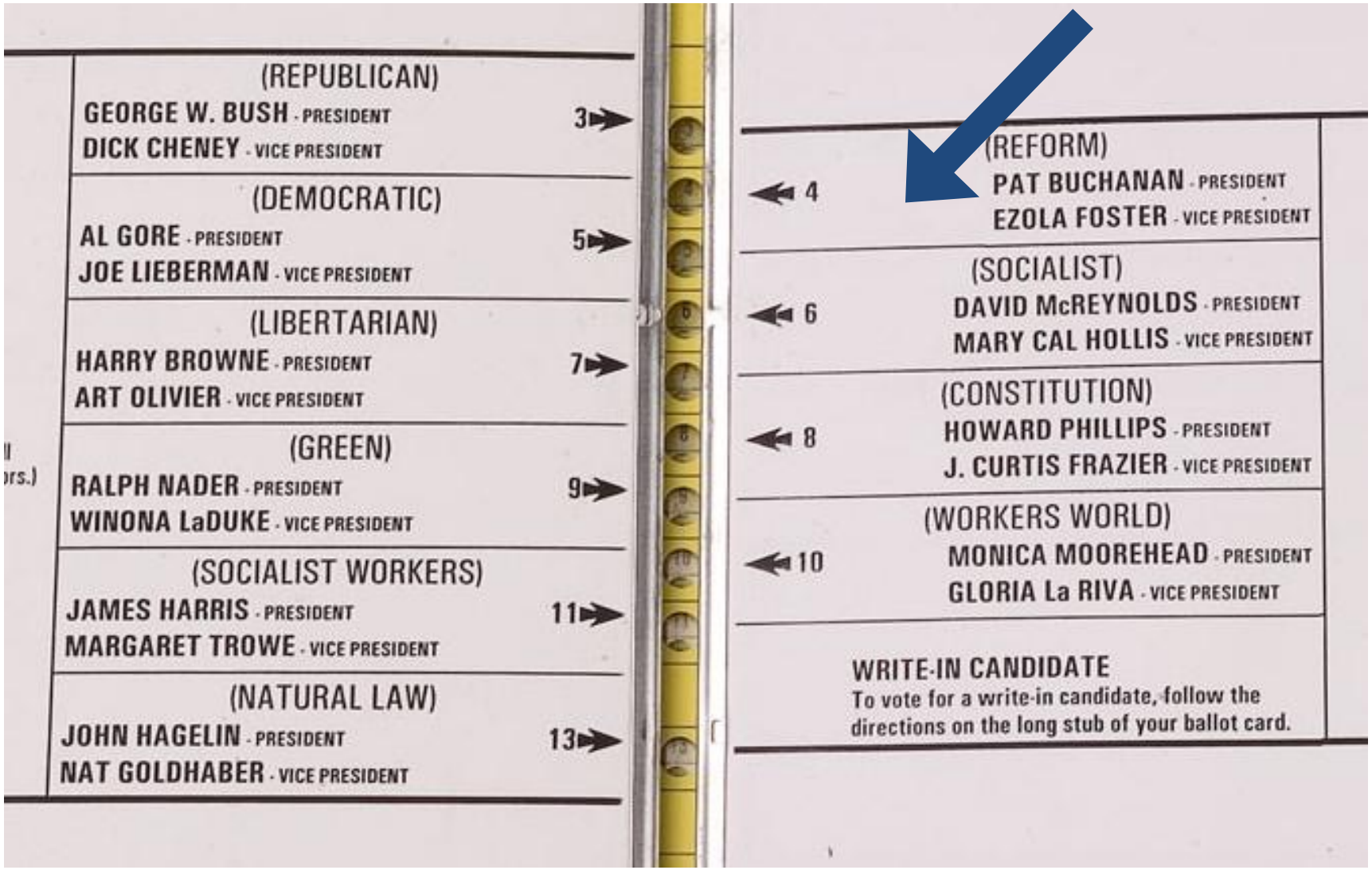
http://americanhistory.si.edu/vote/votingmachine.html

http://americanhistory.si.edu/vote/punchcard.html

Sistemas mecânicos de votação – Florida 2000



Sistemas mecânicos de votação – Florida 2000



http://americanhistory.si.edu/vote/florida.html

Sistemas digitais de votação

Foto: Matt Blaze

http://americanhistory.si.edu/vote/future.html

Urna brasileira

Evolução técnica da urna eletrônica

1996
Intel® 386SX 40Mhz
2MB RAM
Disco 3 1/2 1.44MB

1998
Cyrix Geode GXLV 166MHz
8MB DRAM
Flash card 15MB

2000
Cyrix Geode GXLV 166MHz
8MB DRAM
Flash card 15MB

2002
Cyrix Geode GX1 200MHz
32MB SDRAM
Flash card 16MB

2004
Cyrix Geode GX1 200MHz
64MB DIMM
Flash card 32MB

2006
Cyrix Geode LX700 333MHz
64MB DIMM
Flash card 32MB

2009
Intel® Atom™ Z510P 1.10GHz
512MB DDR2
Flash card 128MB

...

2020
Intel® Atom™ E3940 1.6GHz
4GB DDR3L
2GB M2 SATASoquetada

Segurança – alguns algoritmos utilizados

Criptografia simétrica: AES

Função resumo (resumo criptográfico): SHA-256

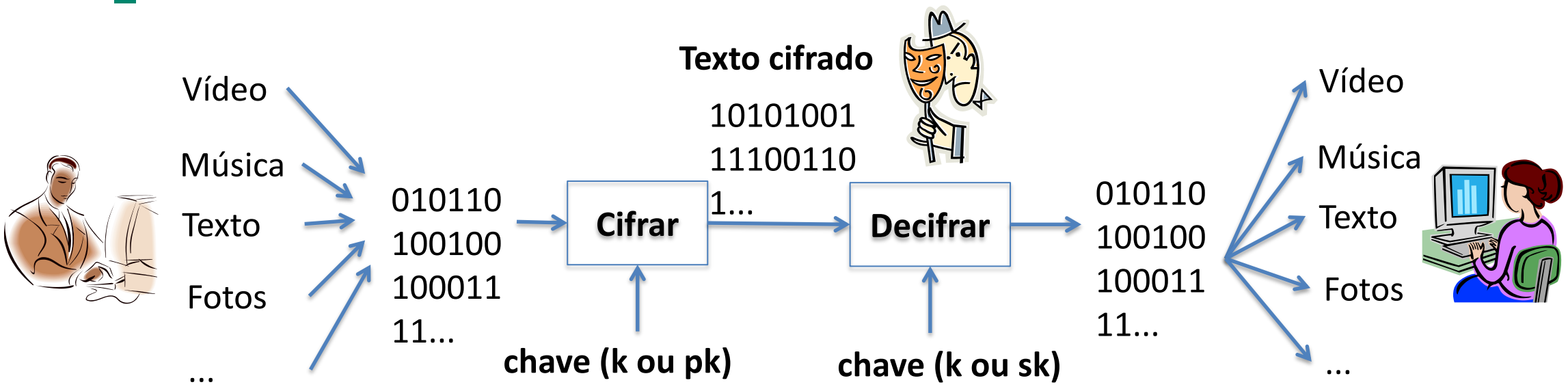
Assinatura digital: RSA e ECDSA

Fonte: Monteiro, J, et al. “Protegendo o sistema operacional e chaves criptográficas numa urna eletrônica do tipo T-DRE. SBSEG, 2019

Segurança - Criptografia

"A arte e ciência de manter informações seguras". - Bruce Scheneier

"Criptografia envolve a projeção de confiança: levar confiança de onde existe para onde é necessária." - Ross Anderson



Segurança – grandes números

O que significa uma chave com 256 bits?

Número de átomos no planeta	$\sim 2^{170}$
Número de átomos no sol	$\sim 2^{190}$
Número de átomos na galáxia	$\sim 2^{223}$
Número de átomos no universo	$\sim 2^{265}$

Número com 256 bits (0 ... 2^{256}-1):

108.389.892.452.648.665.764.138.523.026.027.184.431.003.816.922
.971.289.569.750.251.317.352.717.017.697

Segurança – grandes números

Tempo até a próxima era do gelo	2^{14} anos
Tempo até o sol virar nova	2^{30} anos
Idade do planeta Terra	2^{30} anos
Idade do Universo	2^{34} anos

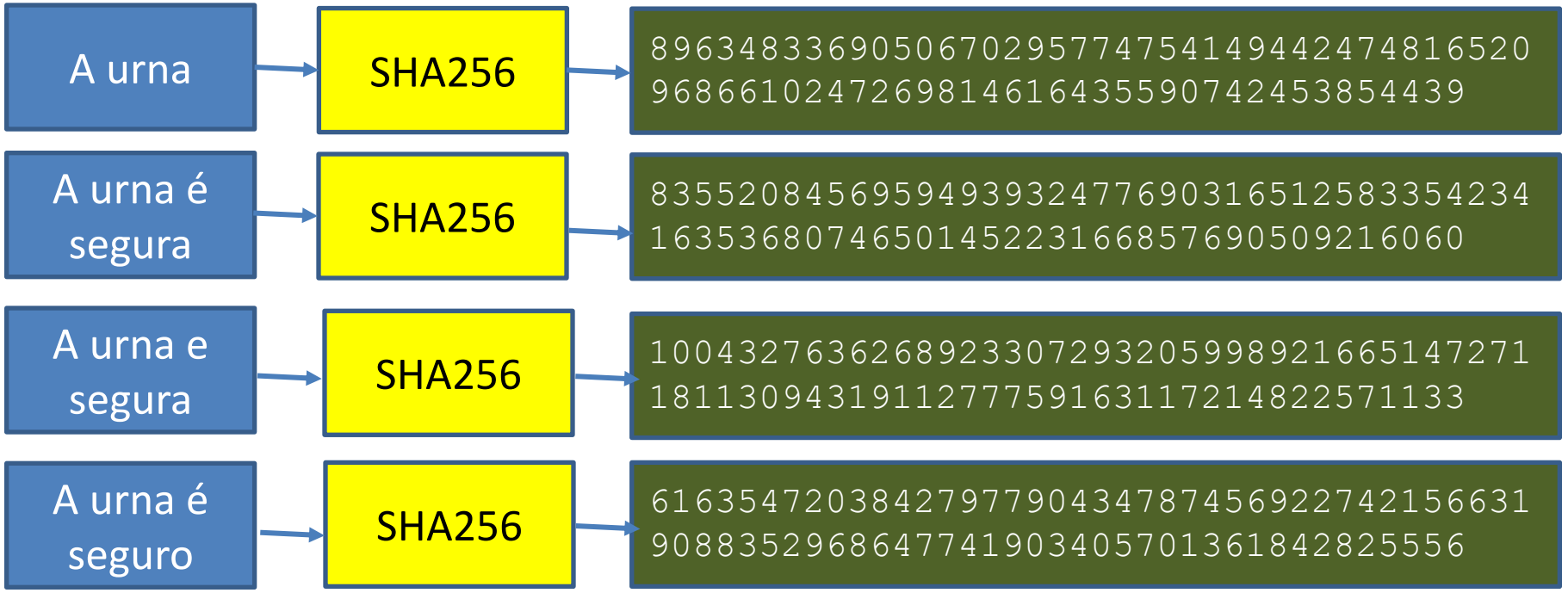
Tempo para quebrar por força bruta
uma chave de 256 bits 2^{192} anos

(Assumindo testar 1 bilhão de chaves em 1ms)

Segurança – resumo criptográfico

Transforma um texto/foto/vídeo/… de qualquer tamanho em um valor de tamanho fixo, por exemplo, um número de 256 bits

Efeito avalanche



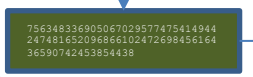
Segurança – Assinatura digital

Honesto

Fontes

Binários

SHA256



assinatura = resumo^{SK} mod N

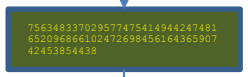
Publicação
Internet TSE

Processo usando RSA simplificado

Fontes

Binários

SHA256



assinatura falsa = resumo^{FK} mod N

Manipulação

resumo = assinatura^{pk} mod N

Confere??

Como saber se isto tudo está funcionando da forma como deveria?

Teste Público de Segurança

Teste de Integridade

Teste de Autenticidade

Teste Público de Segurança

Teste Público de Segurança

"Teste Público de Segurança, também conhecido como TPS, é um evento fixo no calendário eleitoral – previsto na Resolução nº 23.444, do TSE – onde **qualquer brasileiro pode apresentar um plano de ataque aos sistemas eleitorais** envolvidos na geração de mídias, votação, apuração, transmissão e recebimento de arquivos." – Fonte: https://www.justicaeleitoral.jus.br/tps/

Teste Público de Segurança

"O TPS envolve várias etapas, desde a **apresentação dos planos de ataque**, **apresentação do sistema aos investigadores**, **abertura do código** e o **período de ataque propriamente dito**, finalizando meses depois quando o TSE **convida os envolvidos para testar novamente o sistema e verificar se as falhas foram corrigidas.**" – Fonte: https://www.justicaeleitoral.jus.br/tps/

TPS – Linha do tempo

2009 2012 2016 2017 2019

Informações gerais Documentação Notícias Resultados

A primeira edição do Teste Público de Segurança ocorreu durante os dias 10 e 13 de novembro de 2009, com o intuito de buscar a colaboração da sociedade para o aperfeiçoamento da urna eletrônica utilizada nas eleições brasileiras.

Os 37 especialistas em informática e eletrônica que participaram da iniciativa tentaram atacar o sistema eletrônico de votação e encontrar algum tipo de vulnerabilidade.

Notícias e publicações sobre o Teste Público de Segurança (TPS), que terá sua sexta edição realizada entre os dias 22 e 26 de novembro de 2021, no TSE.

TPS LIVE Informações gerais Cronograma Inscrições Documentação

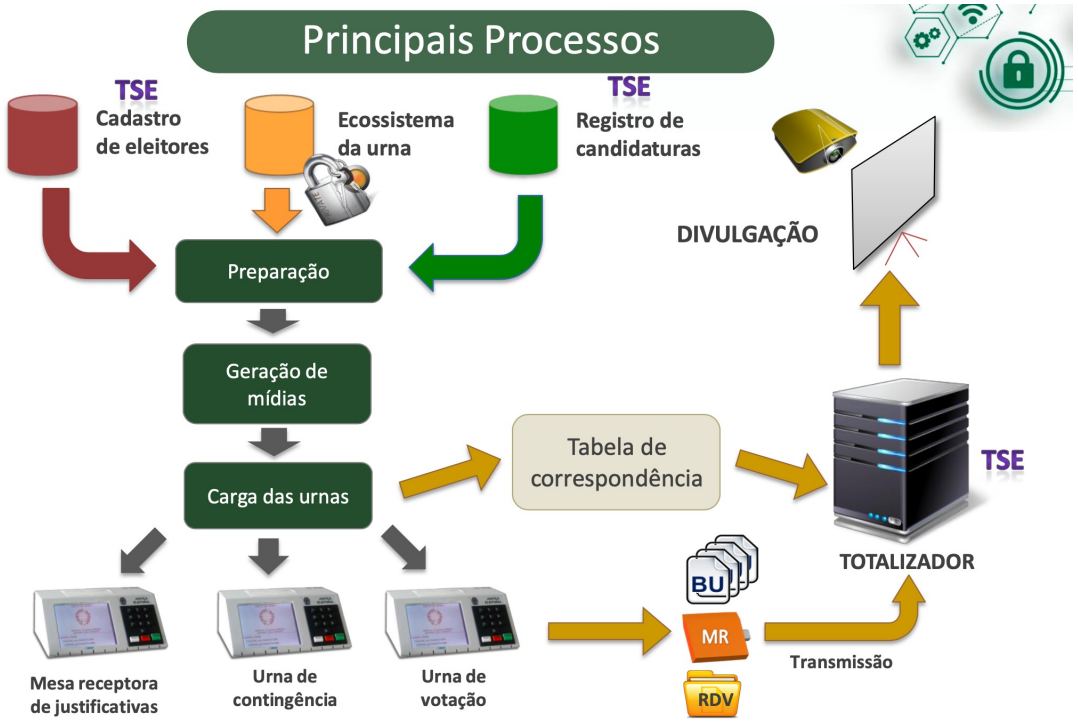
Fonte: https://www.justicaeleitoral.jus.br/tps/

TPS – Quem pode participar?

"Qualquer brasileiro, a partir de 18 anos completos, que atenda aos requisitos do edital do TPS pode participar do teste público." –

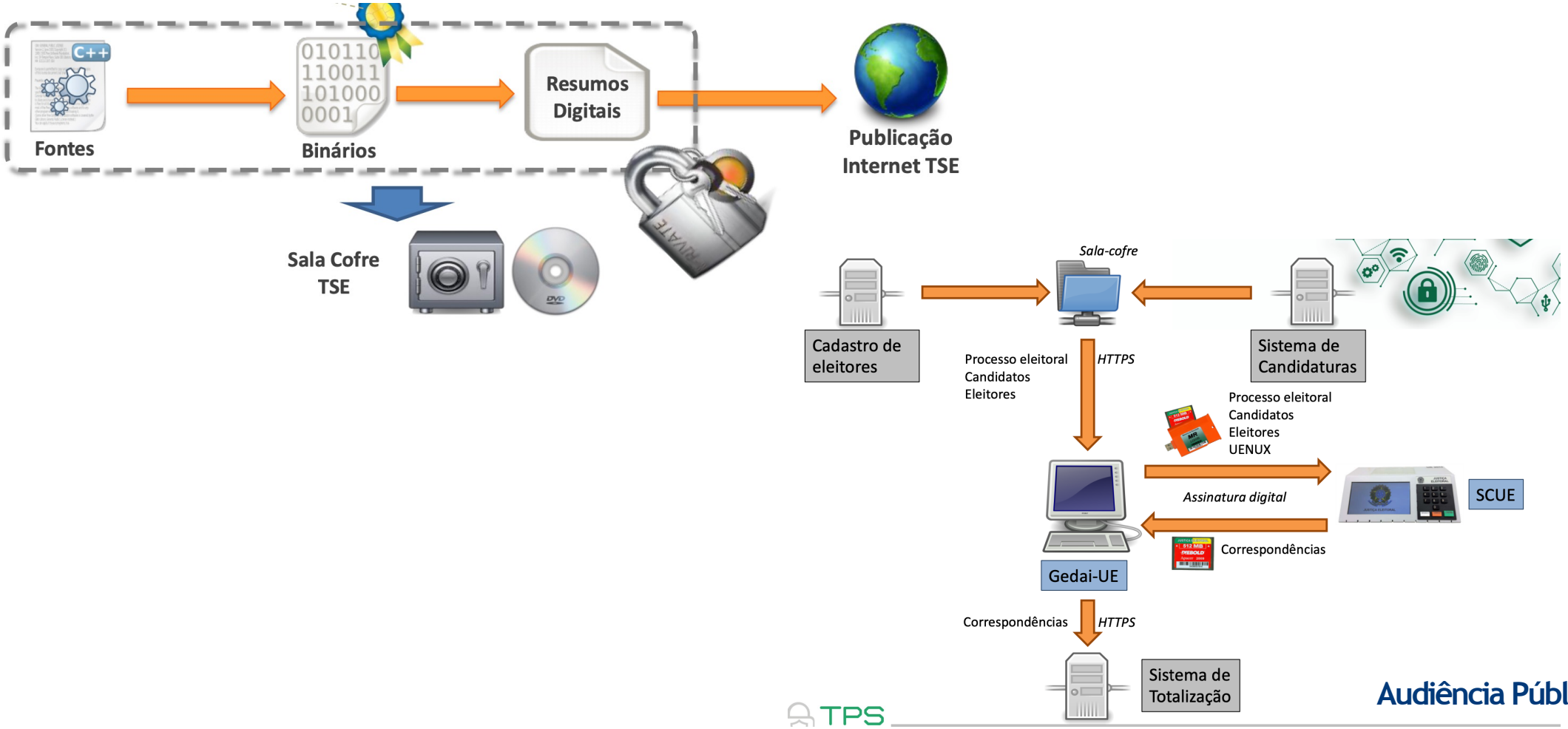
Fonte: https://www.justicaeleitoral.jus.br/tps/

TPS – O que é apresentado?



Fonte: https://www.justicaeleitoral.jus.br/tps/

TPS – O que é apresentado?



Fonte: https://www.justicaeleitoral.jus.br/tps/

TPS – Documentação

Documentos

- Termo de confidencialidade
- Requisição de passagem aérea
- Proposta de concessão de diárias
- Edital TPS 2021
- Resolução nº 23.444, do TSE
- Aviso de Audiência pública
- Relatório Técnico de Avaliação Geral
- Relatório da Comissão Avaliadora

Apresentação explicativa do processo eleitoral brasileiro

- Vídeo explicativo sobre o processo eleitoral brasileiro

Apresentações do vídeo separadas por tema:

- Visão Geral do Processo Eleitoral Brasileiro
- Informações sobre as bibliotecas de integração utilizadas nos sistemas eleitorais
- Informações sobre transmissão e recebimento de arquivos de urna
- Informações sobre os softwares da urna eletrônica
- Informações sobre o Sistema de Segurança – SIS e o JE-Connect
- Informações sobre o hardware da urna eletrônica

Fonte: https://www.justicaeleitoral.jus.br/tps/

https://www.justicaeleitoral.jus.br/tps/

Conclusão

Conclusão

Nenhuma vulnerabilidade durante as eleições foi comprovada.

Sistema **transparente** e em **constante aperfeiçoamento.**

Participação da sociedade em todas as etapas é fundamental.

TSE está indo no caminho certo de **abertura do código-fonte** para além das entidades fiscalizadoras**.**

Ensino de **Computação na Educação Básica**.

Mundo digital → a auditoria é diferente.

https://www.sbc.org.br/noticias/2412-nota-da-sbc-sobre-o-sistema-eletronico-de-votacao-brasileiro

Audiência Pública: A segurança e a transparência do sistema eleitoral brasileiro e a confiabilidade das urnas eletrônicas

Evolução e segurança

Prof. Avelino F. Zorzo – PUCRS e SBC
avelino.zorzo@pucrs.br