HELIOS VOTING NO SISTEMA DE VOTAÇÃO ELETRÔNICA DA UNIOESTE

COMISSÃO TÉCNICA

INTRODUÇÃO

- Helios Voting é um sistema de votação online projetado para garantir a segurança, a transparência e a privacidade em eleições digitais.
- Desenvolvido por uma equipe liderada por Ben Adida, diretor executivo da VotingWorks, especialista em criptografia e segurança da informação.
- Sistema de código aberto, permitindo que pessoas e organizações possam estudar, utilizar e adaptar o sistema para suas necessidades específicas.
- Ideal para contextos como eleições universitárias, onde a facilidade de votação online e a integridade dos resultados são essenciais.

INTRODUÇÃO

- Adaptado pelo Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC), em relação a tradução da linguagem, melhorias de layout, implementação de módulos de autenticação e elaboração de manuais.

- Levantado, estudado e testado por Anibal Diniz e Claudio Roberto Marquetto Mauricio, pensando no uso da Universidade.

- Personalizado pelo NTI da Unioeste, com otimizações relacionadas à layout, importação de dados e disparo de notificações, além da elaboração de manuais.

BENEFÍCIOS DO HELIOS VOTING

1. **Segurança**: Criptografia avançada protege os votos e os resultados contra ataques.

2. **Transparência**: Processo de votação e contagem é auditável e verificável.

3. **Privacidade**: Garante o anonimato dos eleitores, impedindo a identificação dos votos individuais.

4. **Acessibilidade**: Eleitores podem votar remotamente, aumentando a participação e eliminando barreiras geográficas.

BENEFÍCIOS DO HELIOS VOTING

5. **Redução de Fraudes e Manipulações**: Cada etapa é protegida por algoritmos de segurança, aumentando a confiança no resultado final.

6. **Sustentabilidade**: Elimina a necessidade de impressão de cédulas físicas e reduz o uso de recursos materiais.

7. **Eficiência:** Os resultados são obtidos de forma mais rápida, simplificando a contagem e a divulgação.

8. **Confiança na Comunidade Acadêmica:** O uso de tecnologias avançadas reforça a imagem de uma instituição moderna, transparente e preocupada com a segurança de suas eleições.

UTILIZAÇÃO

Diversas Instituições de ensino e pesquisa utilizam o sistema Helios Voting como o sistema padrão votação online, das quais podemos destacar:

- Universidade de São Paulo (USP) - https://sti.fmrp.usp.br/helios-voting-corporativo/
- Universidade de Campinas (UNICAMP) - https://www.pg.unicamp.br/mostra_norma.php?id_norma=10166
- Universidade Federal de Santa Catarina (UFSC) - https://e.ufsc.br/e-democracia-ajuda/
- Universidade Federal de Minas Gerais (UFMG) - https://www.ufmg.br/dti/pagina-inicial/portfolio/servicos/consultas-eleitorais/
- Universidade Federal da Grande Dourados (UFGD) - https://portal.ufgd.edu.br/setor/soc/como-votar
- Universidade Federal de São Carlos (UFSCar) - https://eleicoes.ufscar.br/tutoriais
- Universidade Federal de Pelotas (UFPEL) - https://wp.ufpel.edu.br/famed/2021/04/19/instrucoes-para-votacao-via-sistema-helios-voting/
- Universidade Federal de Alfenas - https://www.unifal-mg.edu.br/eleicoes/sobre-o-sistema-e-o-sigilo-do-voto/
- Fundação Oswaldo Cruz - https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/perguntas_frequentes_versao_021120_1205h1.docx.pdf
- Universidade Federal Rural de Pernambuco - http://www.ufrpe.br/sites/www.ufrpe.br/files/Como%20votar%20no%20Helios%20Voting.pdf
- Instituto Federal do Mato Grosso - https://manuais.ifsp.edu.br/shelves/helios

UTILIZAÇÃO

- Universidade Estadual de Feira de Santana - http://aei.uefs.br/modules/conteudo/conteudo.php?conteudo=64
- Universidade Federal do Rio de Janeiro - https://cartadeservicos.ufrj.br/servico/482
- Instituto Federal do Acre - https://sistemas.ifac.edu.br/helios/
- Universidade de Brasília - http://sintfub.org.br/2020/08/sistema-de-votacao-on-line-e-posto-a-prova-para-eleicao-de-reitor/
- Instituto Federal Sudeste de Minas Gerais - http://www.ufrpe.br/sites/www.ufrpe.br/files/Como%20votar%20no%20Helios%20Voting.pdf
- Instituto Federal de São Paulo - https://manuais.ifsp.edu.br/shelves/helios
- Instituto Federal do Pará (IFPA) - http://2016.dti.ifpa.edu.br/component/k2/itemlist/user/684-2018-08-05-15-48-20
- Instituto Federal de Goiás (IFG) - https://www.ifg.edu.br/component/content/article/138-ifg/pro-reitorias/desenvolvimento-institucional/dti/tecnologia-da-informacao/396-servicos-de-ti?showall=&start=20
- Instituto Federal de Rondônia (IFRO) - https://portal.ifro.edu.br/component/content/article?id=5301
- Instituto Federal de Minas Gerais (IFMG) - https://www.ifmg.edu.br/portal/noticias/eleicoes-do-conselho-superior-sao-transferidas-para-a-proxima-terca-feira-23-de-fevereiro/ManualdoEleitorSistemaHELIOSVOTTING.pdf
- Instituto Federal de Santa Catarina (IFSC) - https://dtic.ifsc.edu.br/sistema-de-votacao-online-helios/
- Instituto Federal Fluminense (IFF) - http://portal1.iff.edu.br/reitoria/noticias/sistema-de-votacao-online-do-iffluminense-garante-rapidez-e-seguranca-dos-processos-eleitorais

ELEIÇÕES REALIZADAS

239 urnas geradas e computadas desde Janeiro de 2022

- **Coordenações de curso:** 54 cursos / 108 urnas
- **Coordenação Local do NUFOPE:** 5 campi / 10 urnas
- **Coordenações de PPG e Residência:** 47 programas / 94 urnas
- **Representante docente de Cascavel no CEPE:** 1 urna
- **Coordenador do Biotério Central de Cascavel:** 1 urna
- **Coordenação do NUPESA de Foz:** 1 urna
- **COREMU HUOP:** 2 urnas
- **Diretor do CCMF de Cascavel:** 2 urnas
- **Diretoria da AFUVEL:** 1 urna
- **Diretoria ADUC:** 1 urna
- **Prêmio professor ADUC:** 5 centros / 5 urnas
- **Centro Acadêmico de Pedagogia de Cascavel:** 1 urna
- **Simulações:** 12 urnas

CRIPTOGRAFIA

- **O que é:**
  - Técnica de proteção de informações através da transformação dos dados em um formato ilegível, a menos que se possua a chave correta para decifrá-los.

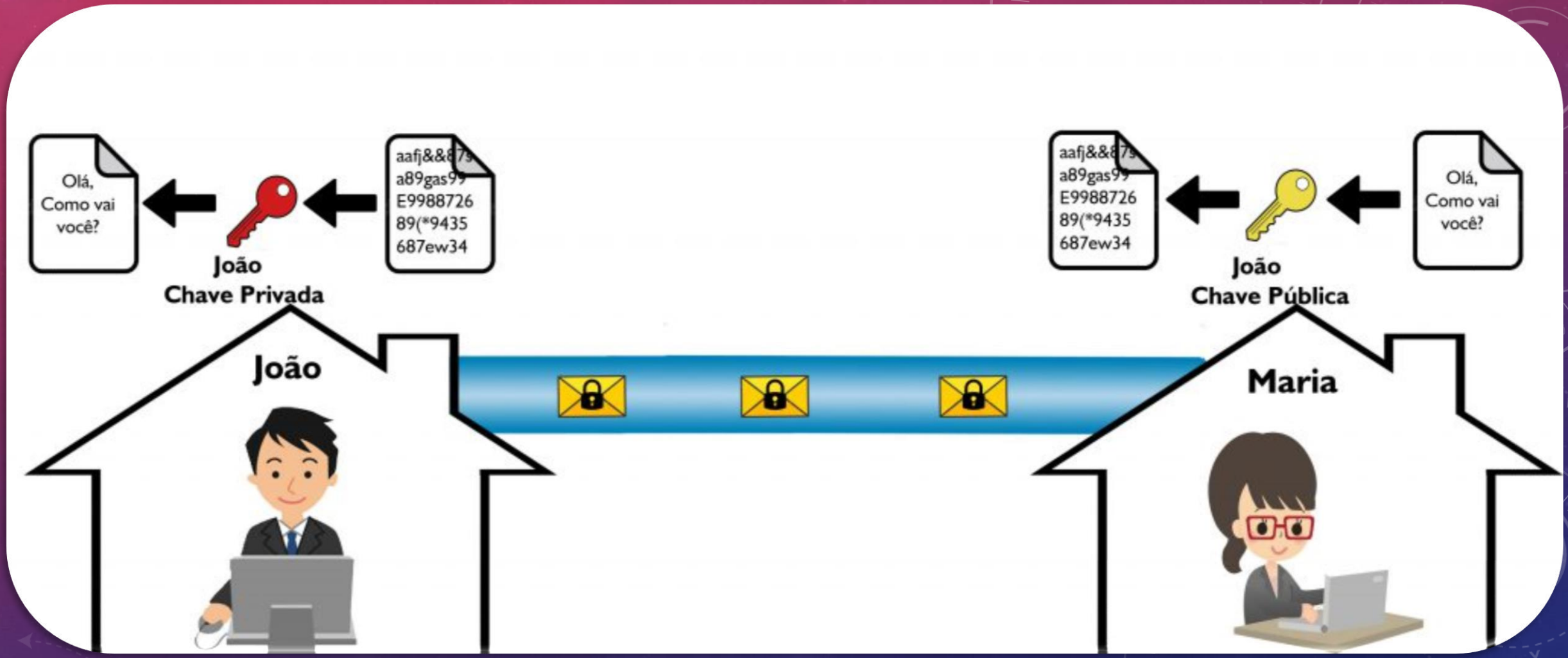
- **Importância da criptografia em eleições digitais:**
  - Assegura a confidencialidade dos votos, a integridade dos resultados e a autenticidade dos eleitores.

CRIPTOGRAFIA

- **Criptografia Assimétrica:**
  - Técnica mais avançada, que utiliza duas chaves distintas, uma para criptografar e outra para descriptografar os dados.

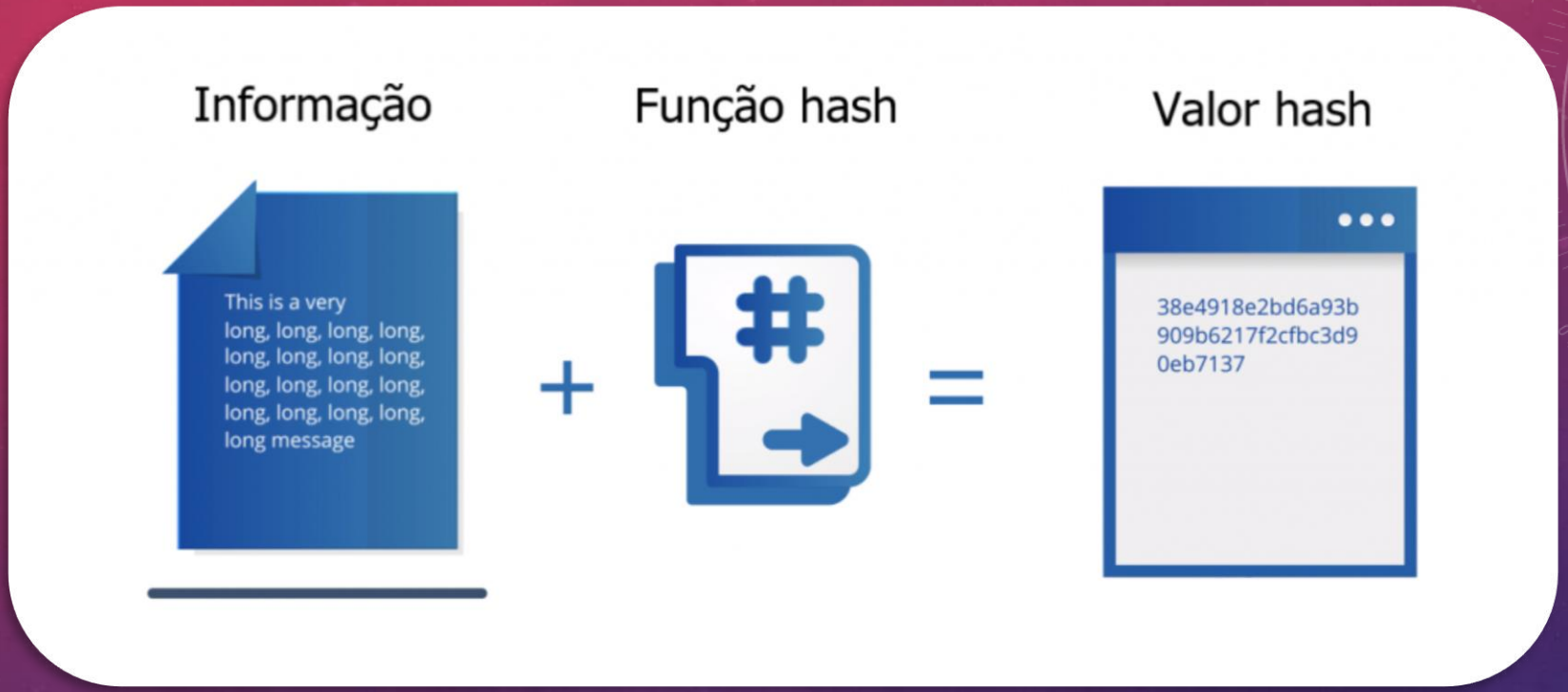
- **Hash:**
  - Técnica que produz uma sequência única irreversível de caracteres a partir de um conjunto de dados, permitindo a comprovação da autenticidade e integridade dos dados.
  - SHA-256: Algoritmo de hash seguro que gera uma sequência de 64 caracteres hexadecimais a partir dos dados de entrada.

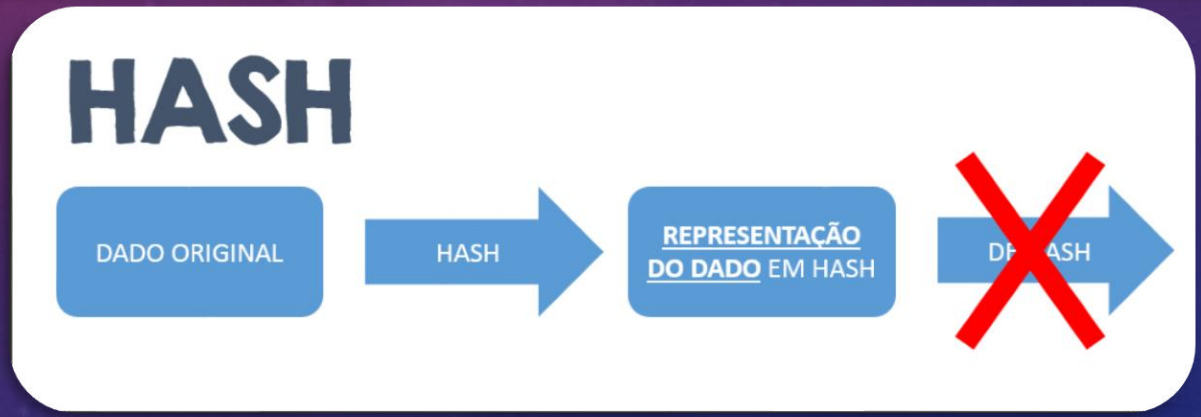
EXEMPLO – CRIPTOGRAFIA ASSIMÉTRICA



Fonte: https://4future.com.br/index.php/2021/10/11/criptografia-chaves-simetricas-e-assimetricas/

EXEMPLOS – HASH





Fontes: https://criptofy.com/hashing-criptomoedas/
https://dba-pro.com/gerenciar-senhas-com-seguranca-no-sql-server/

CRIPTOGRAFIA

- O Helios Voting utiliza técnicas avançadas de criptografia para garantir a segurança e a privacidade dos votos.

- **Criptografia Homomórfica**:
  - Baseia-se no conceito de homomorfismo matemático:
    - Considerando dois grupos (A, .) e (B, *) e uma função F: A->B que toma elementos do conjunto A e retorna elementos do conjunto B. F é um homomorfismo se e somente se F(x . y) = F(x)*F(y) para qualquer par de elementos "x" e "y" pertencentes ao conjunto A.
    - Podemos interpretar o Conjunto A como o dado simples, o conjunto B como o dado criptografado, ‘.’ como as operações que podem ser realizadas no dado simples e ‘*’ como as operações que podem ser realizadas no dado criptografado e F como a função de criptografia.
  - Permite que operações matemáticas sejam realizadas sobre dados criptografados, sem a necessidade de descriptografá-los.
  - O sistema pode executar cálculos diretamente nos votos criptografados, preservando sua privacidade.
  - Importante para a etapa de contagem de votos, onde os votos podem ser processados sem serem expostos.

EXEMPLOS - CRIPTOGRAFIA HOMOMÓRFICA

Fonte: https://www.welivesecurity.com/br/2019/09/06/criptografia-homomorfica-um-esquema-de-criptografia-cada-vez-mais-usado/

CRIPTOGRAFIA

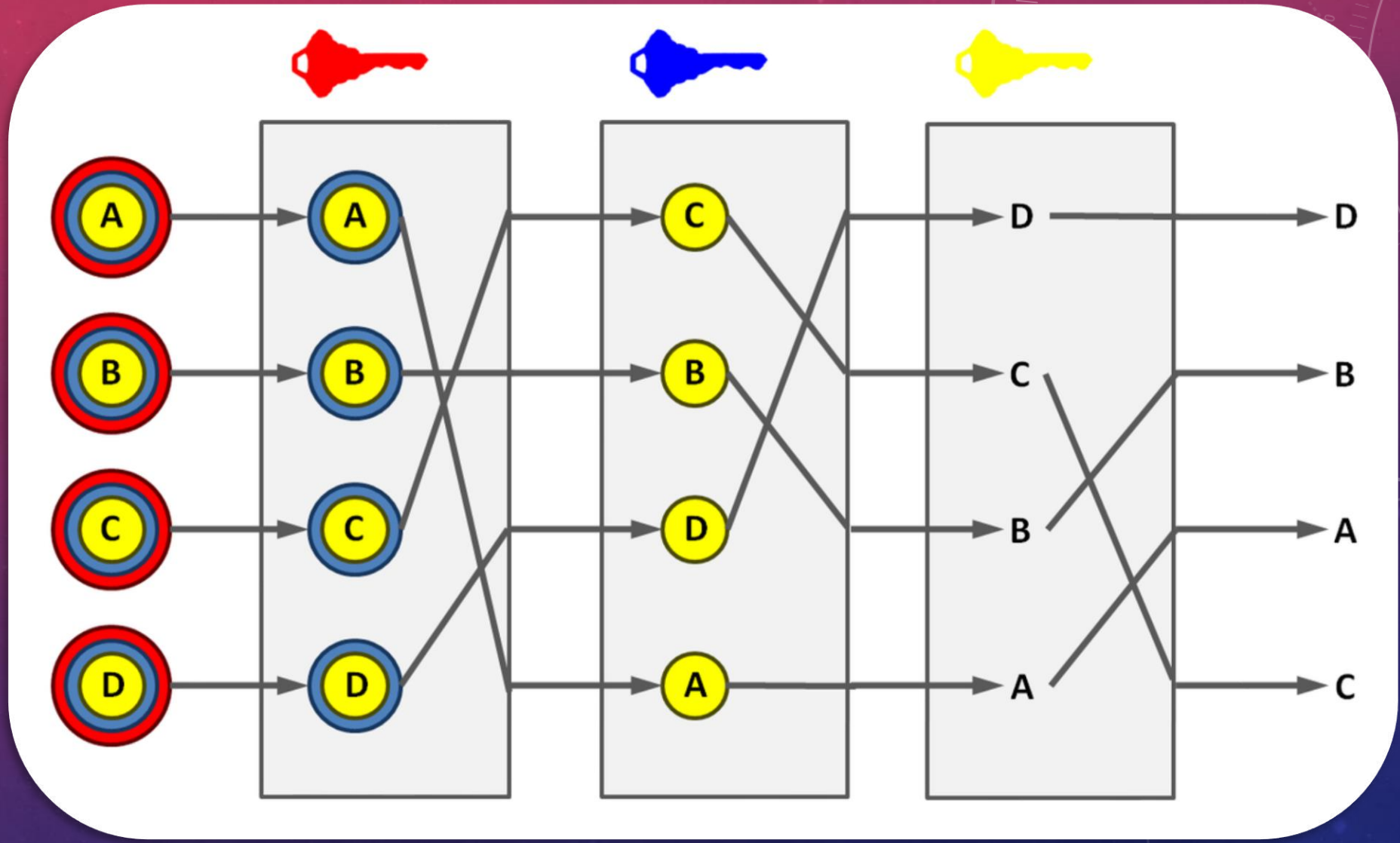
- **Assinatura Cega**:
  - Permite que um usuário assine uma mensagem sem abrir o seu conteúdo.
  - Os eleitores assinam seus votos cegamente, garantindo autenticidade sem revelar suas escolhas.
  - Isso assegura que o voto foi emitido pelo eleitor legítimo, sem comprometer a privacidade do voto.

CONTABILIZAÇÃO DOS RESULTADOS

- O sistema Helios utiliza a técnica de "mix-net" para garantir o anonimato dos votos durante a contagem.

- **Mix-net**:
  - Processo em etapas onde os votos são reordenados e embaralhados de forma segura.
  - Cada servidor "misturador" recriptografa os votos recebidos, embaralhando-os em uma ordem aleatória.
  - Ao final das etapas de mistura, os votos estão completamente embaralhados, mantendo o anonimato.

EXEMPLO - MIX-NET



Fonte: https://en.wikipedia.org/wiki/Mix_network

CONTABILIZAÇÃO DOS RESULTADOS

- **Cálculo dos Votos Misturados:**
  - A criptografia homomórfica é usada para aplicar os cálculos nos votos misturados e obter os resultados.
  - Essa técnica permite a contagem dos votos sem revelar as escolhas individuais dos eleitores.
  - Garante a integridade e autenticidade dos resultados sem comprometer a privacidade.

FUNCIONAMENTO

1. **Fase de Configuração**:
    1. Geração do HASH SHA-256 dos códigos do sistema, para comprovação da integridade durante a eleição.
    2. Definição dos parâmetros de eleição e das opções de voto.

2. **Fase de Votação**:
    1. Dados de acesso são enviados aos e-mails institucionais dos usuários.
    2. Eleitores emitem seus votos de forma anônima e criptografada.
    3. Os votos são assinados cegamente pelo eleitor utilizando a criptografia de assinatura cega.

3. **Fase de Mistura e Contagem**:
    1. Votos criptografados são misturados para garantir anonimato.
    2. Os votos misturados são contabilizados usando a criptografia homomórfica, permitindo a contagem dos resultados sem revelar os votos individuais.

CONCLUSÃO

- O Helios Voting é uma solução confiável para eleições digitais em ambientes universitários.
- Sua abordagem criptográfica garante segurança, privacidade e transparência.
- Estamos comprometidos em oferecer um processo eleitoral moderno e confiável para a nossa comunidade acadêmica.

AGRADECEMOS!

COMISSÃO TÉCNICA

VOTA@UNIOESTE.BR