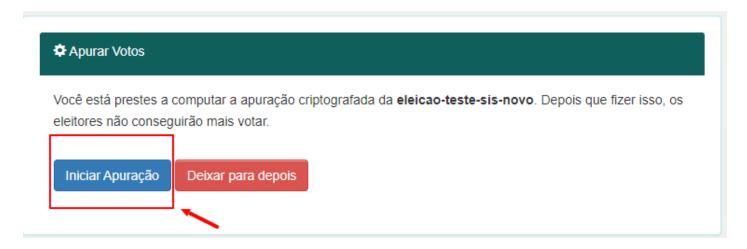
Realizar apuração de eleição com apuradores

Iniciando a apuração:

1 - O administrador da eleição deverá iniciar a apuração clicando em "Iniciar a apuração dos votos, ninguém mais poderá votar";



2 - Ele será direcionado a tela para "Iniciar Apuração";



3 - Será necessário que recarregue a página "F5" ou utilizando botão direito do mouse e "recarregar";

PRÓXIMA ETAPA: A computação da apuração está a caminho. Recarregue essa página em alguns minutos.

4 - Para prosseguir com a apuração será preciso aguardar a ação dos apuradores;

Apurador: Decifrando chave pública para computação dos votos

1 - Acessar o link encaminhado para o seu e-mail;

ATENÇÃO: Você foi designado como apurador da eleição eleicao-teste-sis-novo > Caixa de entrada x

Sistema de Votação da UFLA <vote@votacao.ufla.br>
para mim ▼

Você foi selecionado(a) como apurador(a) da eleicao-teste-sis-novo.

A sua página de apurador pode ser acessada no endereço https://vote.ufla.br/helios/t/eleicao-teste-sis-novo/jsrodrigues@ufla.br/NbP14XhhUYF9

--vote.ufla.br

2 - Clicar em "Decifrar com sua chave";

1 Chave de Apuração

Apurador Juliano Santos Rodrigues eleicao-teste-sis-novo

Você carregou com sucesso sua chave pública.

O código de identificação de sua chave pública é: 1fiRpg+3hIDk/YQ6Pr4GL7eqdYEZk3txN1CmEtlgISU.

Você Pode:

Verificar se você tem a chave privada correta

A apuração criptografada dessa eleição está pronta.

Decifrar com sua chave



Atenção: Você pode verificar se a chave está correta antes de decifrar com sua chave.

3 - Informar a chave;

1 Decifrar Resultado

Apurador

eleicao-teste-sis-novo

Apurador:

@ufla.br

Código de Identificação da Chave Pública: 1fiRpg+3hIDk/YQ6Pr4GL7eqdYEZk3txN1CmEtlg1SU Código de Identificação da Apuração Criptografada: Rijjz86JsNg1Hm25L1rD90xeWVerwHA2jOkn5Egzslo

A apuração criptografada da sua eleição foi computada.

Agora é hora de computar e enviar sua desencriptação parcial.

Esse processo é executado em duas partes.

<u>Primeiro</u>, sua chave privada é utilizada para desencriptar a apuração *dentro* do seu navegador, sem conectar com a rede. Você pode escolher deixar o navegador "offline" para esse passo, se preferir.

<u>Segundo</u>, assim que seus fatores de desencriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor. Se você preferir, você pode computar seus fatores de desencriptação, copiá-los para a área de transferência, reiniciar seu navegador, e pular para o segundo passo, de modo que seu navegador nunca estará online quando você informar sua chave privada.

PRIMEIRO PASSO: informe sua chave secreta

COLAR AQUI A CHAVE PÚBLICA

4 - Clicar em "Gerar minha parte da desencriptação";

PRIMEIRO PASSO: informe sua chave secreta

 $"148874922249631876342824215371860408013040080177434923044817373825719339375687244738471060299150401507840318822060902869386614644588\\ 96494215273989547889201144857352611058572236578734319505128042602372864570426550855201448111746579871811249114781674309062693442442368\\ 6974499706482326218800017095351430479136614328832871500034298023922293615836086866432433497277919762472479486189304238661804105584582\\ 7260662711127004009120307358023890530399447220293078320747239457849850776470319128824954765989999713116613025970060443389123229818234\\ 8403175947450284433411265966789131024573629546048637848902243503970966798589660808533". "b":$

 $"1632863208493301000238405503380545732960161477118595538973916730908621480040646579903858363495375294167564556218249812075026498049238\\ 1375579367675648771293800310370964745767014243638518442553823973482995267304044326777047662957480269391322789378384619428596446446984\\ 6943061876447674624609656225800875643392126317758178959584090166763989756712661796378985576873170761772188432331506951578810612570530\\ 1913307854592898356222139631316962247550981844266104701843626480690102396623671836720471075593589901375030610773800236413791742659573\\ 7403871114187750804346564731250609196846638183903982387884578266136503697493474682071", "q":$

"61329566248342901292543872769978950870633559608669337131139375508370458778917", "y":

 $"100387462914461040194167867040866704012689657488639107552331890075389458123294261472947872068878227698573508777065849409016122423988\\663404581005099657102133263122600126211120311789572715804681795555787814082582941635639739897160347547728985151817547227272745345853\\0080557749171459119176282435573387884939200836886214136338999831561244073385690064431995160801248622785902511959586028472586039639430\\1635459190589315207441640114544847058865111262565026352066419906333924221828435727635423197533462109661287337913226461763602568685054\\36606036667701702756687555063848300433886250948690014296435246886919303837817619037715"], "x":$

"16757288231070942745911934608910102583917738465868643590881148821502581586999"}

Gerar minha parte da desencriptação



pular para o segundo passo

(você precisa já ter computado os fatores de desencriptação.)

5 - Carregar sua desencriptação parcial;

SEGUNDO PASSO: carregar sua desencriptação parcial

Seus fatores de desencriptação parcial e provas foram gerados a seguir.

Sua chave privada foi limpa da memória.

Quando estiver pronto, você pode submeter este resultado ao servidor.

Sua desencriptação parcial:

{"decryption factors":

 $[["14241164715130043947089018880866917925570050666665451526350514778027667019402109130570537251598894775135523166050572014565118173858\\9892799794559314036447486831812904709840089157511413768261128356818967032086764299051666893198206828879649883442414071252752734835649\\4885912019240635734669297481220100603910750631073298841339286475937913832310165416521649383810251597573590742914522452105734026604855\\5750039680773975242006395341237371443259972651819392729220383702420227047670743788796858501629197658292244654012478728955130513858250\\62736501208086323712879021833807556291851786993164615738496915511081473126138260182829"$

 $"447193881339218508413428610167467536156775773586944745084445010796583448008385901301601070961920683289098737317639531361557820817281\\ 5753772443580542343841791280952057496806970349324872018167583245806736176290255045265695376449919411395576158202699779584115886640817\\ 6450501947573490813160160208596526102482992217051620826371585230742971834802770816434949838105005429439924473837496271875296673239947\\ 5466865278811361948193012837210087976894107520672004428662713667106368841357595353735474459189692977330633819583878569249912115009483\\ 0823658515208221962684495566248330757361511185005936998564233321604077836174371974389",$

 $"8484167778620928392363094510677959129563062782656916897153456280477808930048054833765888598030389443383067321156819753704095151810788\\ 1497089373045228862299585852790455565001676058338549232965277100351712518340526107494676312370937353810528959480410721136004009862319\\ 6924154510777932529754783046403838557387211868314987982145669850267622404022725365150008288214467918064641986512285275716706627498584\\ 2086943510948761989501781902409377386691125173807942001481559218520885982716322711389262346435740336477210826548265373875118894291934\\ 088216070867318052265972152786138291759261466391898533862172523901562793856760260385"]], "decryption_proofs": [[("challenge":$

"1306354430440882824010424720208771676878441293836", "commitment": {"A":

Carregar fatores de desencriptação para o servidor

criptação para o scrividor

restaurar e reiniciar o processo de desencriptação

6 - O apurador receberá a informação que sua parte foi realizada.

1 Decifrar Resultado

Apurador .

eleicao-teste-sis-novo

Apurador: @ufla.br

Código de Identificação da Chave Pública: 1fiRpg+3hIDk/YQ6Pr4GL7eqdYEZk3txN1CmEtlglSU Código de Identificação da Apuração Criptografada: Rijjz86JsNg1Hm25LlrD90xeWVerwHA2j0kn5Egzslo

A apuração criptografada da sua eleição foi computada.

Agora é hora de computar e enviar sua desencriptação parcial.

Esse processo é executado em duas partes.

Primeiro, sua chave privada é utilizada para desencriptar a apuração dentro do seu navegador, sem conectar com a rede.

Você pode escolher deixar o navegador "offline" para esse passo, se preferir.

<u>Segundo</u>, assim que seus fatores de desencriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor. Se você preferir, você pode computar seus fatores de desencriptação, copiá-los para a área de transferência, reiniciar seu navegador, e pular para o segundo passo, de modo que seu navegador nunca estará online quando você informar sua chave privada.

Pronto!

Voltar para eleição

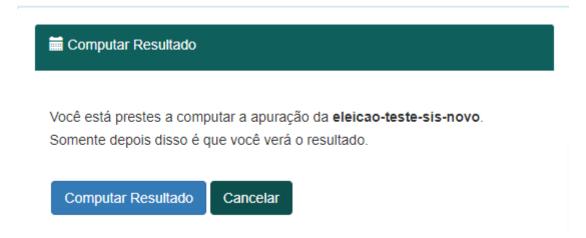
Continuando com a apuração

1 - Após os procedimentos dos apuradores, o Administrador já consegue Computar o resultado, para isto basta clicar em "Combinar a Desencriptação dos Apuradores e Computar o Resultado";

PRÓXIMA ETAPA: Combinar a Desencriptação dos Apuradores e Computar o Resultado

As partes desencriptadas de cada apurador serão combinadas e a apuração será computada. Depois de fazer isso, a apuração estará visível apenas para você, o administrador da eleição.

2 - Clicar em "Computar Resultado";



3 - O resultado será mostrado abaixo.



SIM 1 NÃO 0 VOTO EM BRANCO 0

VOCE APROVOU O NOVO SISTEMA DE VOTAÇÃO?

Criado Fri, Nov 17, 2023 6:51 AM por JULIANO SANTOS RODRIGUES Atualizado Fri, Nov 17, 2023 4:44 PM por JULIANO SANTOS RODRIGUES