

Descriptografar apuração

Quando a urna entrar na fase de apuração, você deverá visitar seu painel de apurador para descriptografar a sua parte da contagem de votos. Para essa finalidade **você vai precisar do arquivo com a sua chave secreta** que você baixou quando configurou suas chaves criptográficas.

1) Acesse o seu painel de apurador. acione o botão **Descriptografar minha parte**. Você será levado para a tela **Descriptografar o Resultado**.

The screenshot shows the 'Descriptografar o Resultado' interface. At the top, there is a green header with the 'INSTITUTO FEDERAL' logo and navigation links: 'Início', 'Admin', 'Ajuda', and 'Sobre'. On the right side of the header, it displays 'Usuário: Fulano de Tal' and a 'Sair' button. The main content area has a title 'Eleição para Coordenador Exemplo' with a back arrow icon. Below the title, it says 'Apurador - Fulano de Tal'. A light blue box contains the following text: 'A contagem criptografada para esta eleição está pronta. Para que o processo de apuração continue, realize a descriptografia da sua parte. Para isso você utilizará sua chave secreta.' Below this text is a green button labeled 'Descriptografar minha parte'. Below the light blue box, a green box shows a success message: 'Você enviou com sucesso sua chave pública!'. Below this, a light blue box displays the public key: 'A impressão digital da sua chave pública é: PLdNsFGImM1JqGqMrJVmcpc59kTpNqhQPPj3xqg6Oj8'. At the bottom, under the heading 'Se desejar, você pode:', there is a green button labeled 'Verificar se possui a chave secreta correta'.

O processo é realizado em dois passos. **A interface é visualmente semelhante entre os dois passos, leia atentamente as informações em tela para se orientar sobre o seu progresso.**

Eleição para Coordenador Exemplo

Apurador - Fulano de Tal - Descriptografar o Resultado

Apurador: @ifap.edu.br

Impressão digital da chave pública: PLdNsFGImM1JqGqMrJVmcp59kTpNqhPPj3xqg60j8

Impressão digital da contagem criptografada: sckRW+LoyHPCpoNIs4dLeg/S4attMTB0wEf10IE4HcI

A contagem criptografada para a sua eleição foi computada.

Agora é hora de computar e enviar a sua parte da descriptografia.

Este processo é performed em dois passos.

Primeiro, sua chave secreta é usada para descriptografar a contagem *dentro* do navegador, sem se conectar à rede. Você pode escolher deixar o seu navegador offline para este passo se desejar.

Segundo, quando seus fatores de descriptografia estiverem calculados, seu navegador precisará estar online para enviá-los ao servidor. Se desejar, você pode calcular seus fatores de descriptografia, copiá-los para sua área de transferência, reiniciar seu navegador e pular para o segundo passo para que seu navegador nunca fique online no momento em que entrar sua chave secreta.

2) Desça a tela até o bloco do primeiro passo. Neste passo, abra o arquivo contendo a sua chave secreta, copie todo o conteúdo e cole no campo disponível, então acione o botão **Gerar descriptografia parcial**. Você será levado para o segundo passo.

Este processo é performed em dois passos.

Primeiro, sua chave secreta é usada para descriptografar a contagem *dentro* do navegador, sem se conectar à rede. Você pode escolher deixar o seu navegador offline para este passo se desejar.

Segundo, quando seus fatores de descriptografia estiverem calculados, seu navegador precisará estar online para enviá-los ao servidor. Se desejar, você pode calcular seus fatores de descriptografia, copiá-los para sua área de transferência, reiniciar seu navegador e pular para o segundo passo para que seu navegador nunca fique online no momento em que entrar sua chave secreta.

PRIMEIRO PASSO: entre sua chave secreta

```
{ "public_key": { "g":  
  "14887492224963187634282421537186040801304008017743492304481737382571933937568724473847106029915040150784031882206090286938661464458  
  896494215273989547889201144857352611058572236578734319505128042602372864570426550855201448117465798718112491147816743090626934424423  
  68697449970648232621880001709535143047913661432883287150003429802392229361583608686643243349727791976247247948618930423866180410558  
  4582726066271127004009120307358023890530399447220293078320747239457849850776470319128824954765989999713116613025970060443389123229  
  8182348403175947450284433411265966789131024573629546048637848902243503970966798589660808533", "p":  
  "1632863208493301000550338054573296016  
  23813755793676756003103709647457670  
  44698469430618764000365622580087564  
  57053019133078545928003562221396313189022475  
  26595737403871114137750804346564731250609196  
  "613295662483429012925438727699789508706335  
  "5835124332807483715965907538608909382195097  
  4701450546426875667443242203308482021799359  
  18407744974538701091088423844298754914053712  
  3099926065746957619423301764379673438007856
```

3 Gerar descriptografia parcial

[pular para o segundo passo](#)

(você precisa já ter calculado seus fatores de descriptografia.)

3) No segundo passo, você verá um grande campo de texto, já preenchido com a sua descriptografia. Basta acionar o botão **Enviar fatores de descriptografia para o servidor**. Você verá uma mensagem de progresso, e por fim um alerta de sucesso.

Segundo, quando seus fatores de descryptografia estiverem calculados, seu navegador precisará estar online para enviá-los ao servidor. Se desejar, você pode calcular seus fatores de descryptografia, copiá-los para sua área de transferência, reiniciar seu navegador e pular para o segundo passo para que seu navegador nunca fique online no momento em que entrar sua chave secreta.

SEGUNDO PASSO: enviar sua descryptografia parcial

Seus fatores de descryptografia parciais e provas foram gerados abaixo.
Sua chave secreta foi limpa da memória.
Quando estiver pronto, você pode enviar esse resultado ao servidor.

Sua descryptografia parcial:

```
0151894200409104572420009448442583618052152699451782126216357853734934353644299328252878928953574532313222651354073305544229109727
18260739341889170786601088052869198728724302121554610421701587063556167786842512101476697968707352550478921342156256230515686026713492
568815326669972798471524893716790612368700786229840926931374296419491977149457802834"}, "response":
"3878347352477820637083458425075424553799373269244648565650005232529379981589"}, {"challenge":
"5269377908474148898989650375638678611448060291878", "commitment": {"A":
"88532546195270905207449410205710382975431765891161175486852991988583442232342730148593883451739753291816209477885580790185445155040
83894753556536741547373583759248050541737238083910679647064696444193664076770570829067365317178230674478671134745235320013393082228
539128403829457217640658812646231036280557985749959713593503178776226786672396818928594754145710368169709002272948174169298840094823
688088251808071145345339145605301007908192508004630993923507768740581526926500756957993143161935774208039546692115895949171961200528
70065489848583458730942769655417142740684080591466457463199517622798813954290144485131450", "B":
"14231535479594022455950848732496769567553136180612509257958072366937740240171745775102235714807603086786584286772170039233082667801
0719451304725717265444709123022672384122710025085887809190750313077272729439687255870225639333833592616325805104323604004064279583
751788843672977243027793986738015288359152912641728676883632239305743849122368687898132491196571192023777892169354419754715295728390
2709714867094573449863974634317950281811927986348718862112869300859773652301620097679218210516948359529913570771974646816988487793179
0472763546862080058962107356899060130022298202981525035197964362595392409303487070230572"}, "response":
"9333921600455861697922301078582446432271480511542173234758872538582084287688"}]]}
```

Enviar fatores de descryptografia para o servidor

[redefinir e reiniciar o processo de descryptografia](#)

Eleição para Coordenador Exemplo

Apurador - Fulano de Tal - Descryptografar o Resultado

Apurador: @ifap.edu.br

Impressão digital da chave pública: PLdNsFGImM1JqGqMrJVmcp59kTpNqhPPj3xqg60j8

Impressão digital da contagem criptografada: sckRW+LoyHPCpNI54dLeg/S4attMTBOWEf10IE4HcI

A contagem criptografada para a sua eleição foi computada.
Agora é hora de computar e enviar a sua parte da descryptografia.

Este processo é performed em dois passos.

Primeiro, sua chave secreta é usada para descryptografar a contagem *dentro* do navegador, sem se conectar à rede.
Você pode escolher deixar o seu navegador offline para este passo se desejar.

Segundo, quando seus fatores de descryptografia estiverem calculados, seu navegador precisará estar online para enviá-los ao servidor.
Se desejar, você pode calcular seus fatores de descryptografia, copiá-los para sua área de transferência, reiniciar seu navegador e pular para o segundo passo para que seu navegador nunca fique online no momento em que entrar sua chave secreta.

Enviando e verificando seus fatores de descryptografia e provas...

Eleição para Coordenador Exemplo

Apurador - Fulano de Tal - Descryptografar o Resultado

Apurador: @ifap.edu.br

Impressão digital da chave pública: PLdNsFGImM1JqGqMrJVmcp59kTpNqhPPj3xqg60j8

Impressão digital da contagem criptografada: sckRW+LoyHPCpNI54dLeg/S4attMTBOWEf10IE4HcI

A contagem criptografada para a sua eleição foi computada.
Agora é hora de computar e enviar a sua parte da descryptografia.

Este processo é performed em dois passos.

Primeiro, sua chave secreta é usada para descryptografar a contagem *dentro* do navegador, sem se conectar à rede.
Você pode escolher deixar o seu navegador offline para este passo se desejar.

Segundo, quando seus fatores de descryptografia estiverem calculados, seu navegador precisará estar online para enviá-los ao servidor.
Se desejar, você pode calcular seus fatores de descryptografia, copiá-los para sua área de transferência, reiniciar seu navegador e pular para o segundo passo para que seu navegador nunca fique online no momento em que entrar sua chave secreta.

✓ Feito! Ir ao painel da eleição

Pronto! Você realizou com sucesso a descryptografia da sua parte na apuração de votos.
Você verá no seu painel um alerta de sucesso.

INSTITUTO FEDERAL
de Brasília

[Início](#) [Admin](#) [Ajuda](#) [Sobre](#)

Usuário: Fulano de Tal [Sair](#)

[<](#)  **Eleição para Coordenador Exemplo****Apurador - Fulano de Tal** **Você enviou com sucesso sua descryptografia!** **Você enviou com sucesso sua chave pública!** A impressão digital da sua chave pública é: **PLdNsFGImM1JqGqMrJVmcpc59kTpNqhqPPj3xqg6Oj8****Se desejar, você pode:** **Verificar se possui a chave secreta correta**

Revisão #4

Criado 2025-08-04 13:15:01 UTC por Felipe de Freitas Fernandes

Atualizado: 2025-10-01 19:29:49 UTC por Felipe de Freitas Fernandes