

MANUAL DO USUÁRIO

IFCRYPT



Elaborado por Anderson Fostinger da Silva

CAMPINAS

2021

SUMÁRIO

1. INTRODUÇÃO	3
2. GERAR CHAVES	4
3. CRIPTOGRAFIAR	8
4. DESCRIPTOGRAFIAR.....	12

1. INTRODUÇÃO

O IFCrypt foi desenvolvido como parte do Trabalho de Conclusão de Curso (TCC) do curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de São Paulo (IFSP) – Campus Campinas para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas.

O IFCrypt é uma ferramenta para criptografar e descriptografar arquivos em formato PDF para serem enviados de forma a garantir a confidencialidade, integridade, autenticidade e o não-repúdio dos arquivos transmitidos via internet.

Em resumo, o IFCrypt funciona da seguinte forma: o usuário ao iniciar a aplicação precisa gerar um par de chaves caso ainda não possua. Após isso, seleciona-se a função Criptografar ou Descriptografar. A função Criptografar recebe como entrada um arquivo e duas chaves. O arquivo é cifrado com uma chave exclusiva para ele, gerada pelo sistema, que por sua vez, é cifrada com a chave pública do destinatário. E por fim, o arquivo é assinado e pode ser enviado. A função Descriptografar realiza o processo inverso, verificando a assinatura digital e decifrando o arquivo.

A tela exibida ao iniciar a aplicação pode ser vista na imagem abaixo. Nela há três botões para acessar as funcionalidades da aplicação: **Gerar Chaves**, **Criptografar** e **Descriptografar**.



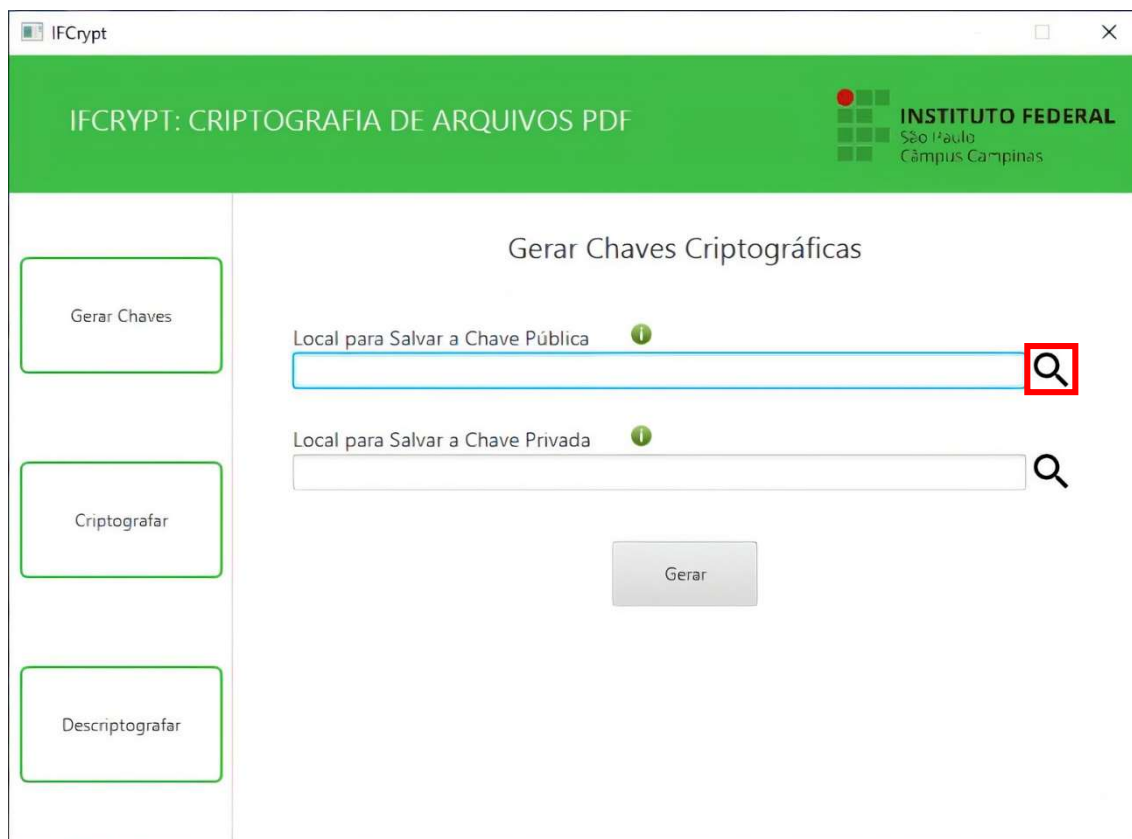
2. GERAR CHAVES

Ao iniciar a aplicação, o usuário precisa gerar um par de chaves se ainda não possuir. O usuário que já tiver um par de chaves, geradas pelo sistema, pode avançar para a seção 3 ou 4 que explica, respectivamente, como criptografar e descriptografar um arquivo PDF. As chaves são geradas utilizando o algoritmo criptográfico RSA e são utilizadas para assinar o arquivo e cifrar a chave exclusiva de cada arquivo no momento da criptografia.

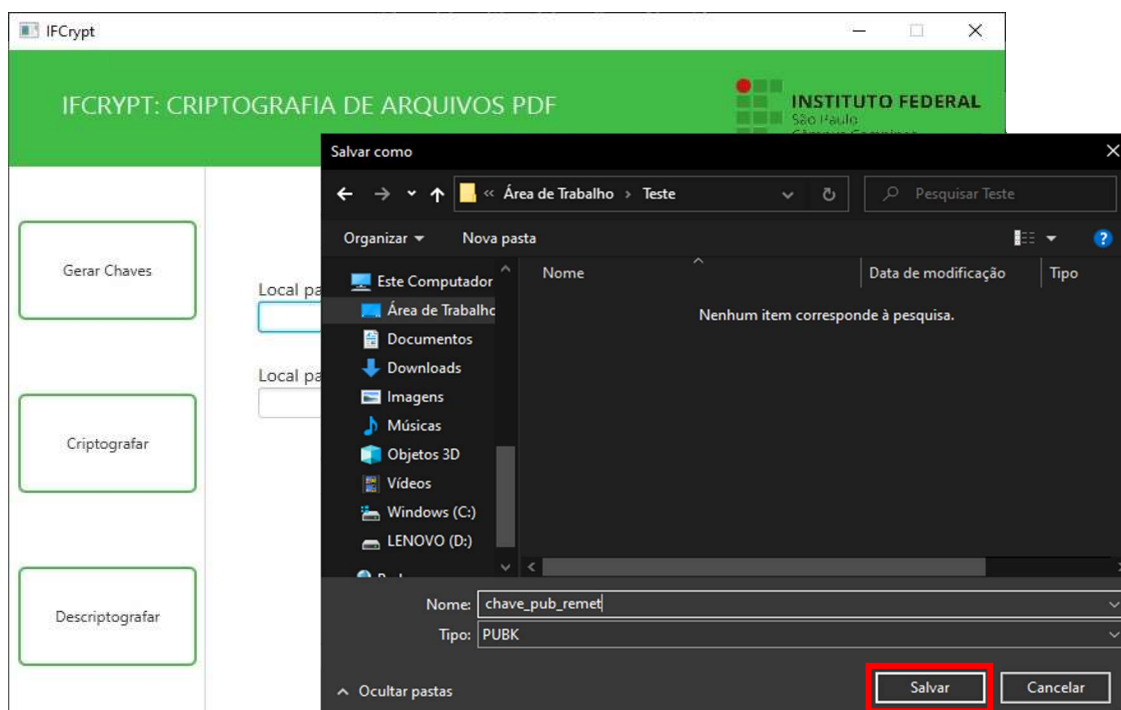
The screenshot displays the IFCrypt application window. The title bar reads 'IFCrypt'. The header bar is green and contains the text 'IFCRYPT: CRIPTOGRAFIA DE ARQUIVOS PDF' on the left and the logo of 'INSTITUTO FEDERAL São Paulo Câmpus Campinas' on the right. The main content area is titled 'Gerar Chaves Criptográficas'. On the left side, there is a vertical sidebar with three buttons: 'Gerar Chaves', 'Criptografar', and 'Descriptografar'. The 'Gerar Chaves' button is highlighted with a green border. In the main area, there are two input fields. The first is labeled 'Local para Salvar a Chave Pública' with a green information icon (i) and a search icon (Q). The second is labeled 'Local para Salvar a Chave Privada' with a green information icon (i) and a search icon (Q). Below these fields is a 'Gerar' button.

A geração das chaves deve ser feita de acordo com os seguintes passos:

1. Clique na imagem da lupa;



2. Na janela que abrir, escolha o nome da chave e o local onde será salva e clique em **Salvar**;



3. Realize novamente os passos 1 e 2 para preencher o campo **Local para Salvar a Chave Privada**;
4. Após todos os campos preenchidos, clique no botão **Gerar**;

IFCrypt

IFCRYPT: CRIPTOGRAFIA DE ARQUIVOS PDF

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Gerar Chaves Criptográficas

Gerar Chaves

Local para Salvar a Chave Pública ⓘ

C:\Users\ander\Desktop\Teste\chave_pub_remet.pubk 🔍

Local para Salvar a Chave Privada ⓘ

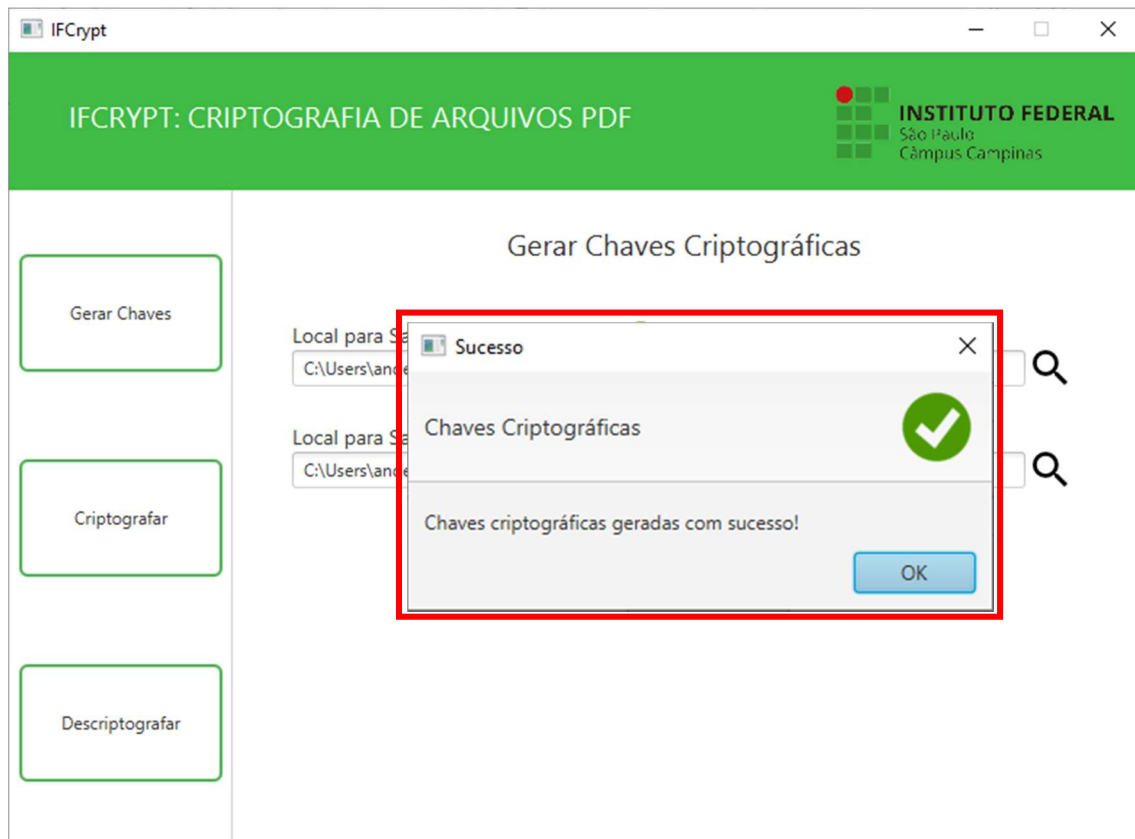
C:\Users\ander\Desktop\Teste\chave_priv_remet.privk 🔍

Gerar

Criptografar

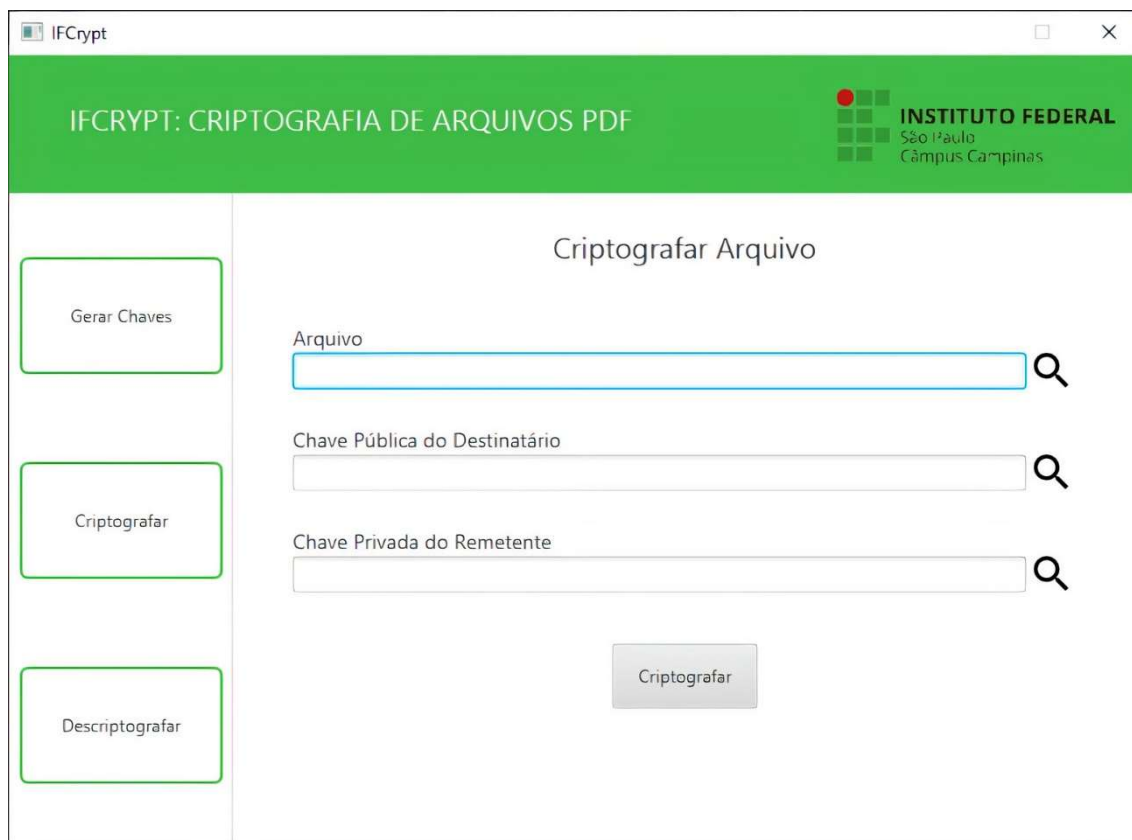
Descriptografar

5. O sistema gera as chaves, salva nos locais informados no Passo 2 e exibe a mensagem abaixo.



3. CRIPTOGRAFAR

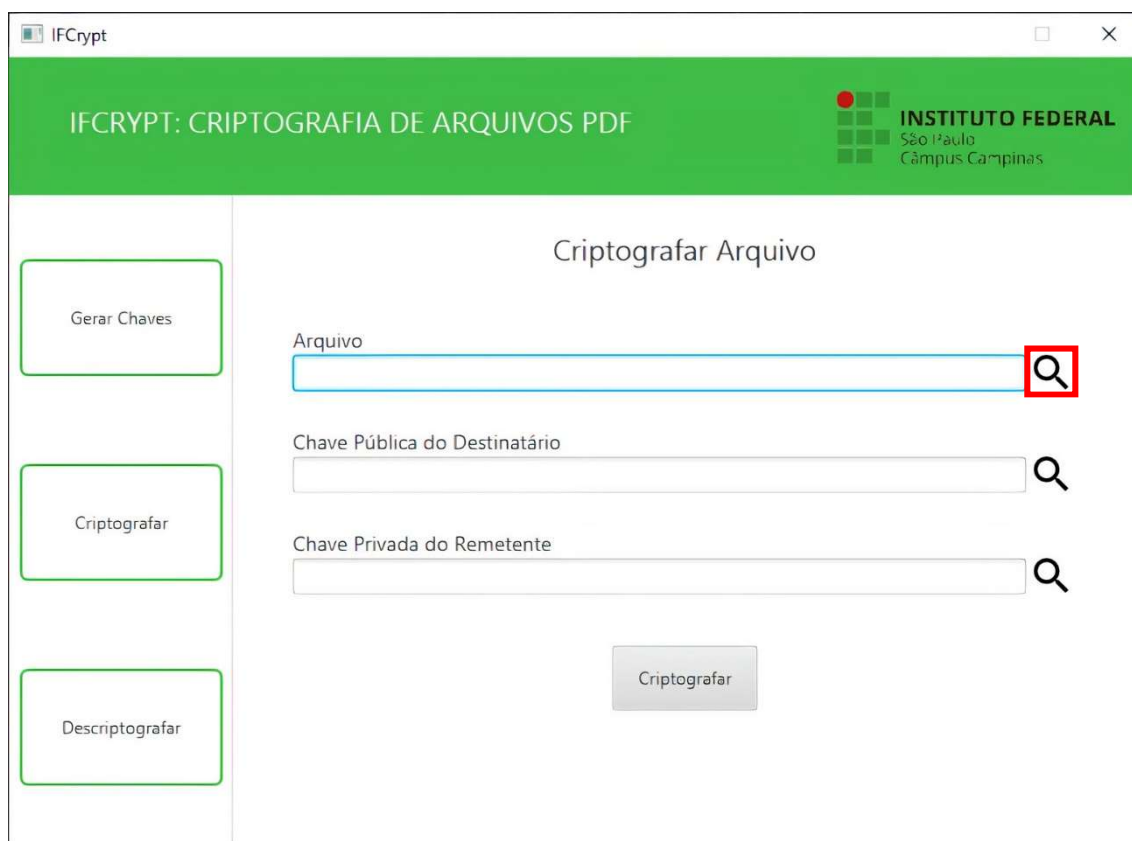
A função Criptografar cifra o arquivo PDF e salva com a extensão IFC. Nesta funcionalidade, a chave exclusiva de cada arquivo, utilizada para cifrá-lo, é gerada utilizando o algoritmo criptográfico AES e esta mesma chave é cifrada com a chave pública do destinatário do arquivo.



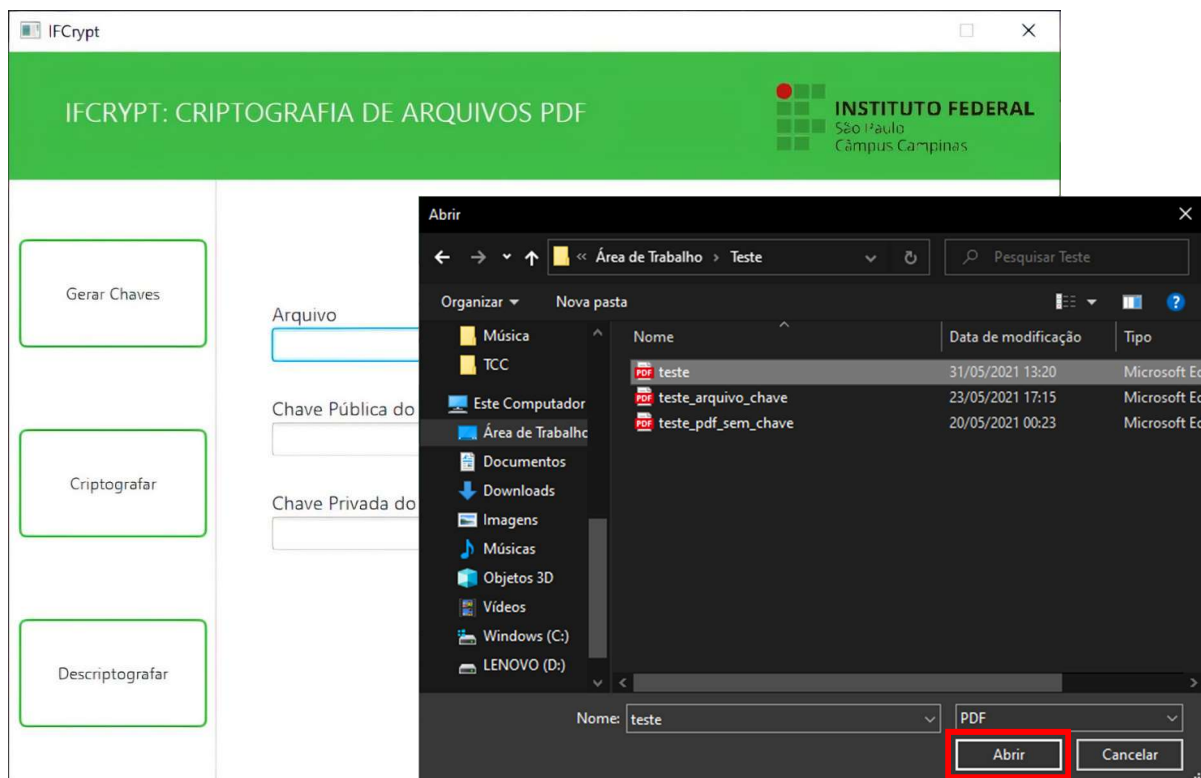
The screenshot shows the IFCrypt web application interface. The title bar indicates the application is 'IFCrypt'. The header is green and contains the text 'IFCRYPT: CRIPTOGRAFIA DE ARQUIVOS PDF' and the logo of the 'INSTITUTO FEDERAL São Paulo Câmpus Campinas'. The main content area is titled 'Criptografar Arquivo'. On the left, there is a sidebar with three buttons: 'Gerar Chaves', 'Criptografar', and 'Descriptografar'. The main area contains three input fields, each with a search icon: 'Arquivo', 'Chave Pública do Destinatário', and 'Chave Privada do Remetente'. A 'Criptografar' button is located at the bottom center of the main area.

O usuário que deseja criptografar um arquivo PDF precisa realizar os seguintes passos:

1. Clique na imagem da lupa;



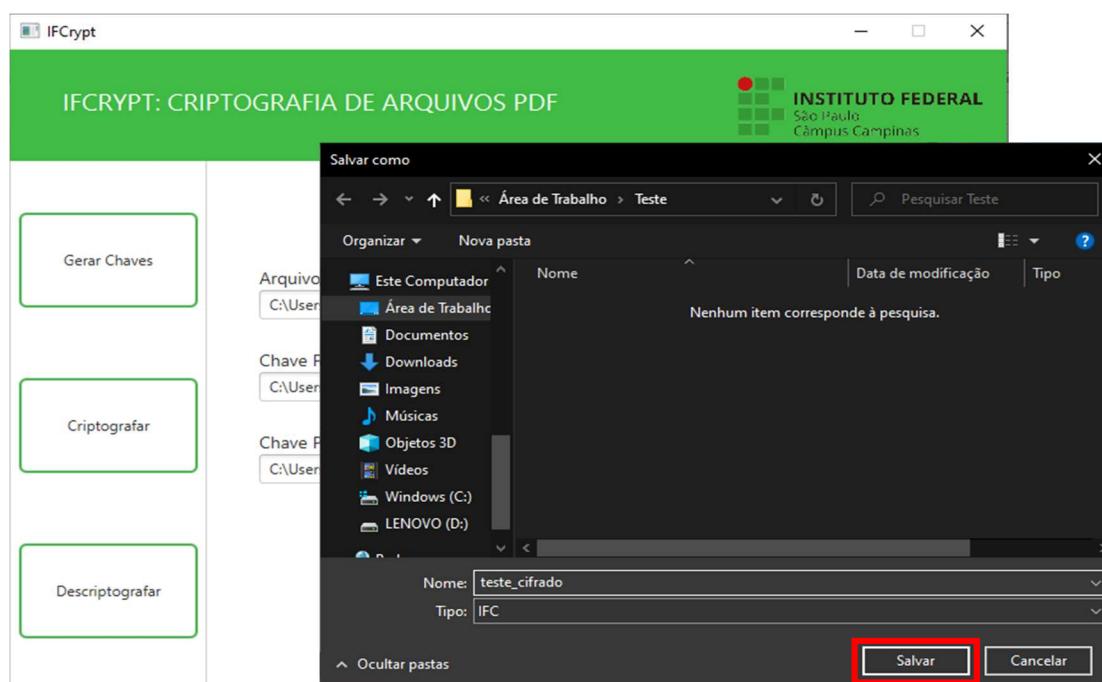
2. Na janela que abrir, escolha o arquivo de acordo com o campo que será preenchido e clique em **Abrir**;



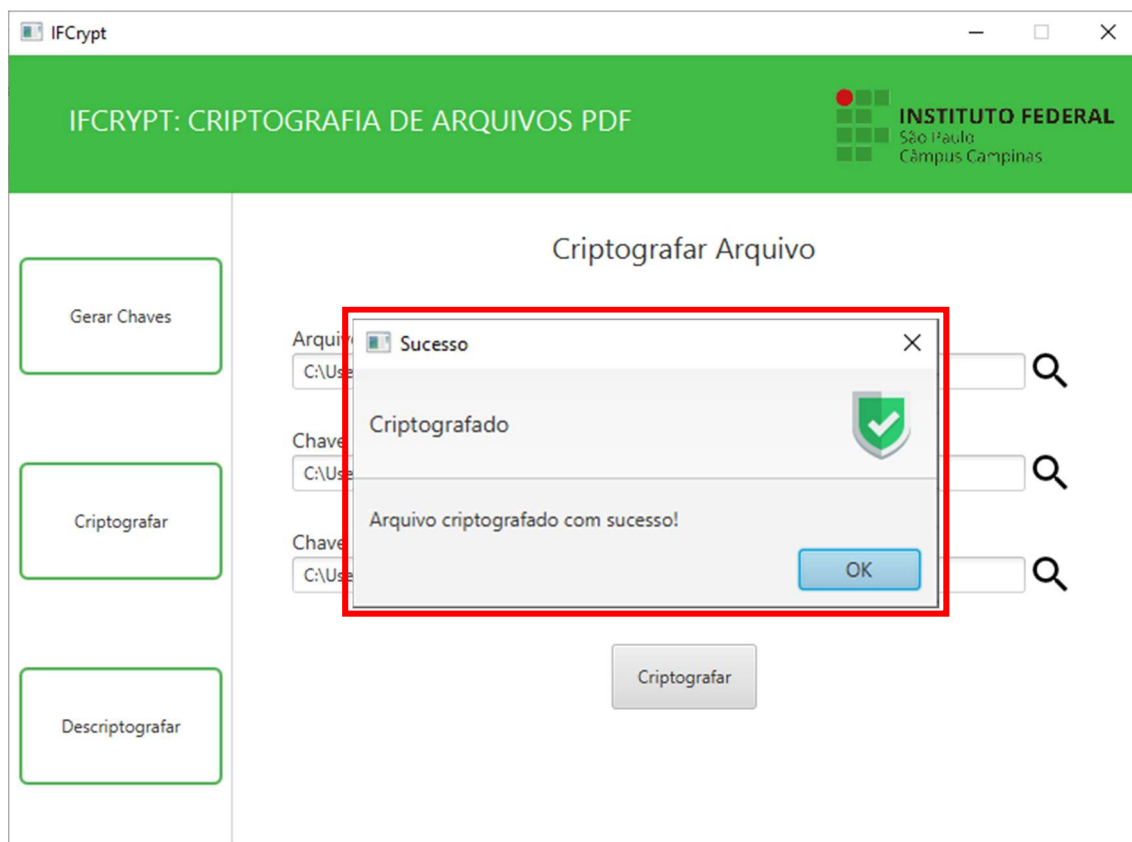
3. Realize novamente os passos 1 e 2 para preencher os campos **Chave Pública do Destinatário** e **Chave Privada do Remetente**;
4. Após todos os campos preenchidos, clique no botão **Criptografar**;



5. Após clicar no botão Criptografar, informe o nome e o local onde o arquivo criptografado será salvo e clique em **Salvar**;



6. O sistema criptografa e salva o arquivo no local informado pelo usuário no passo 5 e exibe a mensagem abaixo.



4. DESCRIPTOGRAFAR

A função Descriptografar decifra o arquivo IFC e salva em formato PDF.

The screenshot shows a web application window titled 'IFCrypt'. The header is green and contains the text 'IFCRYPT: CRIPTOGRAFIA DE ARQUIVOS PDF' and the logo of 'INSTITUTO FEDERAL São Paulo Câmpus Campinas'. The main content area is titled 'Descriptografar Arquivo'. On the left, there is a sidebar with three buttons: 'Gerar Chaves', 'Criptografar', and 'Descriptografar'. The 'Descriptografar' button is highlighted with a green border. In the main area, there are three input fields, each with a search icon (magnifying glass) to its right: 'Arquivo Criptografado', 'Chave Pública do Remetente', and 'Chave Privada do Destinatário'. Below these fields is a button labeled 'Descriptografar'.

O usuário que deseja descriptografar um arquivo IFC precisa realizar os seguintes passos:

1. Preencha todos os campos, seguindo as mesmas etapas descritas nos passos 1 e 2 da seção 3;



IFCrypt

IFCRYPT: CRIPTOGRAFIA DE ARQUIVOS PDF

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Descriptografar Arquivo

Gerar Chaves

Criptografar

Descriptografar

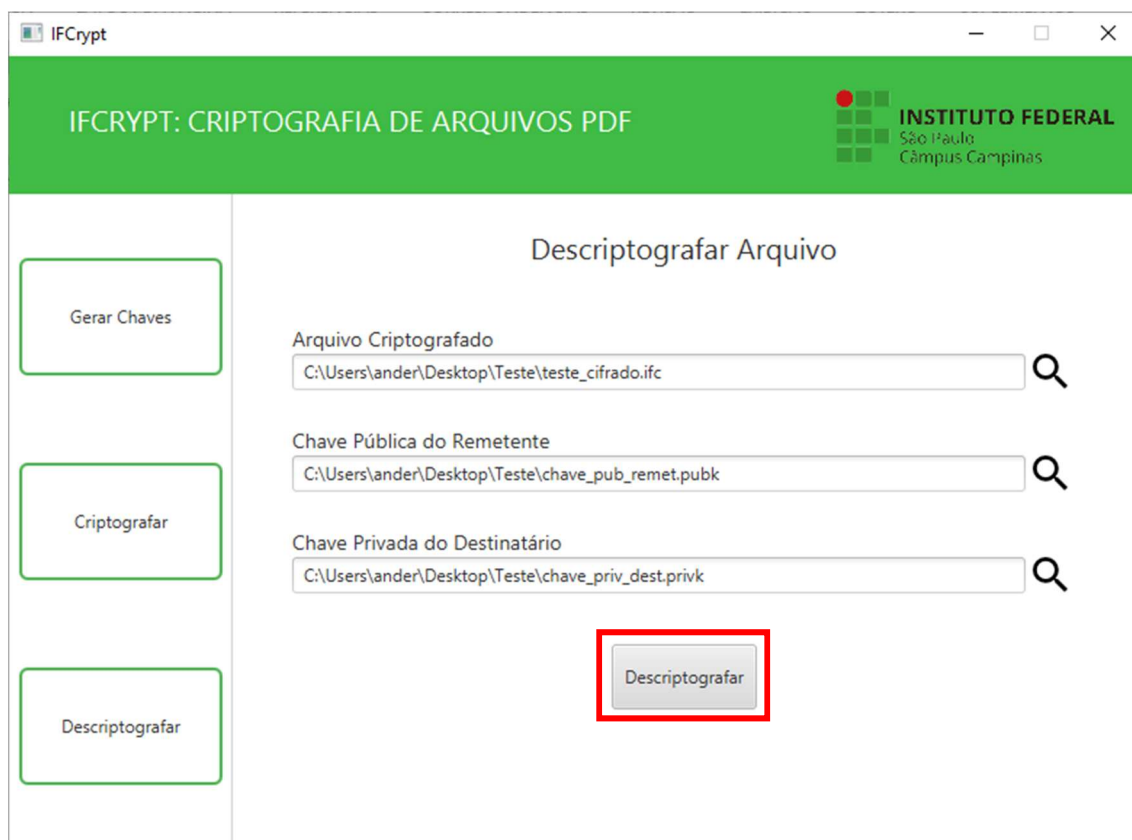
Arquivo Criptografado
C:\Users\ander\Desktop\Teste\teste_cifrado.ifc

Chave Pública do Remetente
C:\Users\ander\Desktop\Teste\chave_pub_remet.pubk

Chave Privada do Destinatário
C:\Users\ander\Desktop\Teste\chave_priv_dest.privk

Descriptografar

2. Após todos os campos preenchidos, clique no botão **Descriptografar**;



IFCrypt

IFCRYPT: CRIPTOGRAFIA DE ARQUIVOS PDF

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Descriptografar Arquivo

Gerar Chaves

Criptografar

Descriptografar

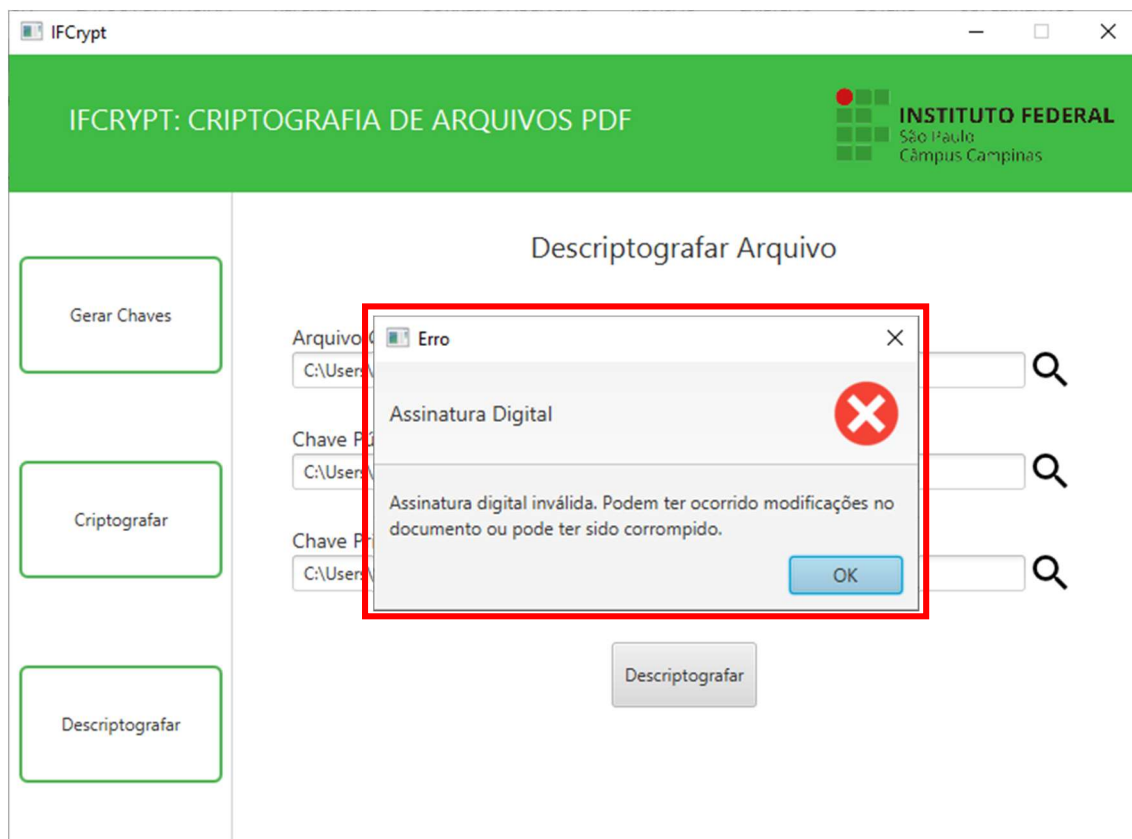
Arquivo Criptografado
C:\Users\ander\Desktop\Teste\teste_cifrado.ifc

Chave Pública do Remetente
C:\Users\ander\Desktop\Teste\chave_pub_remet.pubk

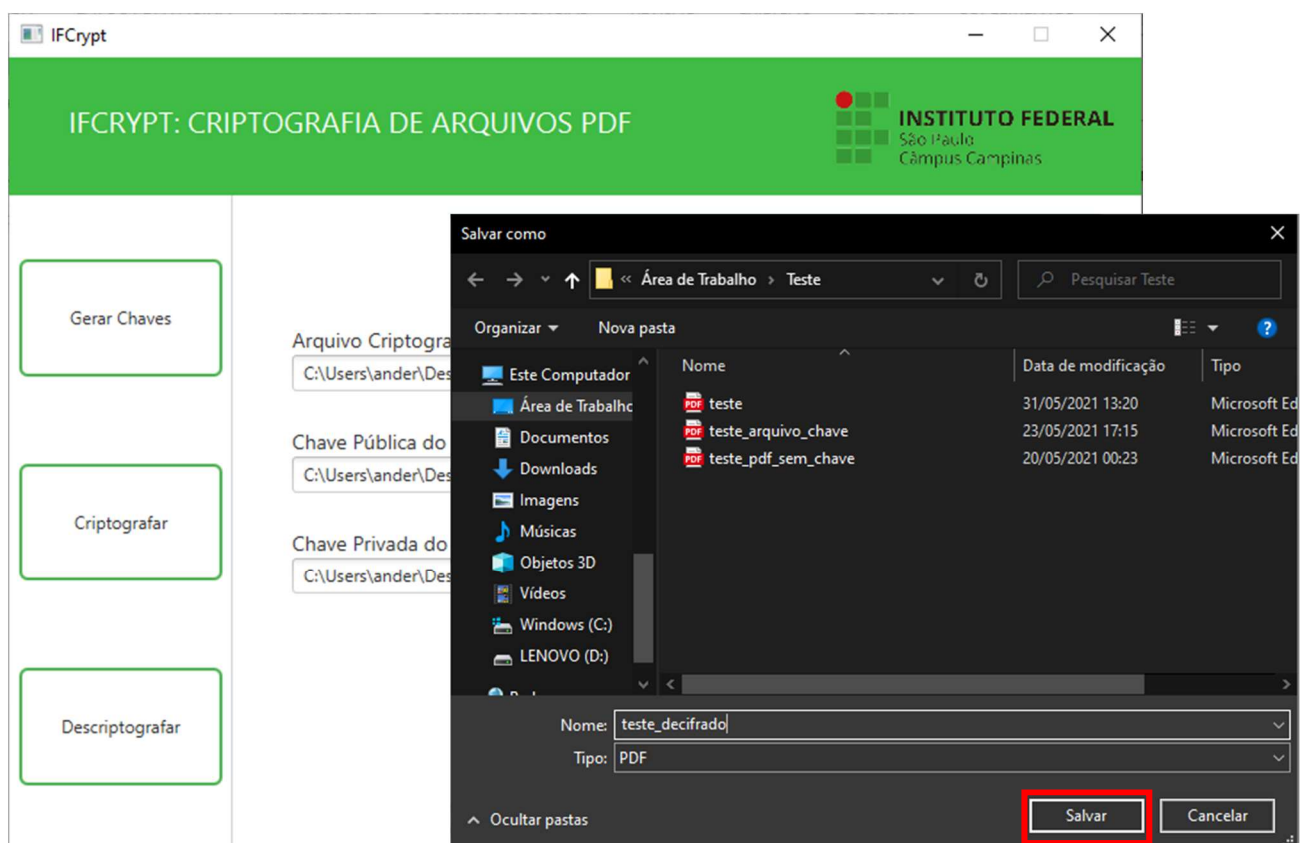
Chave Privada do Destinatário
C:\Users\ander\Desktop\Teste\chave_priv_dest.privk

Descriptografar

3. O sistema verifica a validade da assinatura digital, que foi anexada ao arquivo no processo de criptografia, se a assinatura não for válida é exibida a mensagem abaixo informando ao usuário que o arquivo pode ter sofrido alguma modificação ou pode ter sido corrompido. Neste caso, o arquivo não é processado. Se a mensagem não for exibida, vá para o passo 4;



4. Após o sistema confirmar a validade da assinatura digital, uma janela é aberta. Informe nesta janela o nome e o local onde o arquivo descriptografado será salvo e clique em **Salvar**;



5. O sistema descriptografa e salva o arquivo no local informado pelo usuário no passo 4 e exibe a mensagem abaixo.

