

# Manual RbCripto

## **Sobre o RbCripto**

O RbCripto é um programa simples que foi concebido com fins acadêmicos. É capaz de realizar a encriptação e deciptação de arquivos usando o moderno conceito de curvas elípticas combinado ao algoritmo Diffie-Hellman e associado ao algoritmo de chave simétrica AES 256bits.

## **Requisitos**

O programa é constituído apenas por um pequeno executável com menos de 1MB e não requer instalação, ou seja, pode ser mantido em *pendrive* ou cartão de memória. Seu funcionamento não requer mais que 10MB de memória. Para encriptar ou deciptar arquivos, requer memória e espaço em disco de acordo com o tamanho do arquivo. Por exemplo: para um arquivo de 30MB, requer os mesmos 30MB de espaço em disco e preferencialmente os 30MB de memória RAM. Para grandes arquivos, por exemplo, 5GB, precisa dos 5GB de espaço em disco e quanto mais memória livre, melhor. O RbCripto possui um algoritmo para aperfeiçoar a alocação de memória, evitando-se assim a paginação (situação em que o sistema utiliza espaço em disco quando não houver muita memória livre).

## **Estatísticas de exemplo**

O RbCripto foi testado em um computador baseado no processador AMD X2 1.9GHz com 1GB de RAM e HD SATA2. Para um arquivo com 4,2GB (tamanho de um DVD caseiro), precisou de 12 minutos para realizar a encriptação e nove para a deciptação. Para este trabalho, usou cerca de 700MB RAM livres. Para um arquivo com 300MB, foi necessário 1 minuto e meio para encriptar e meio para deciptar.

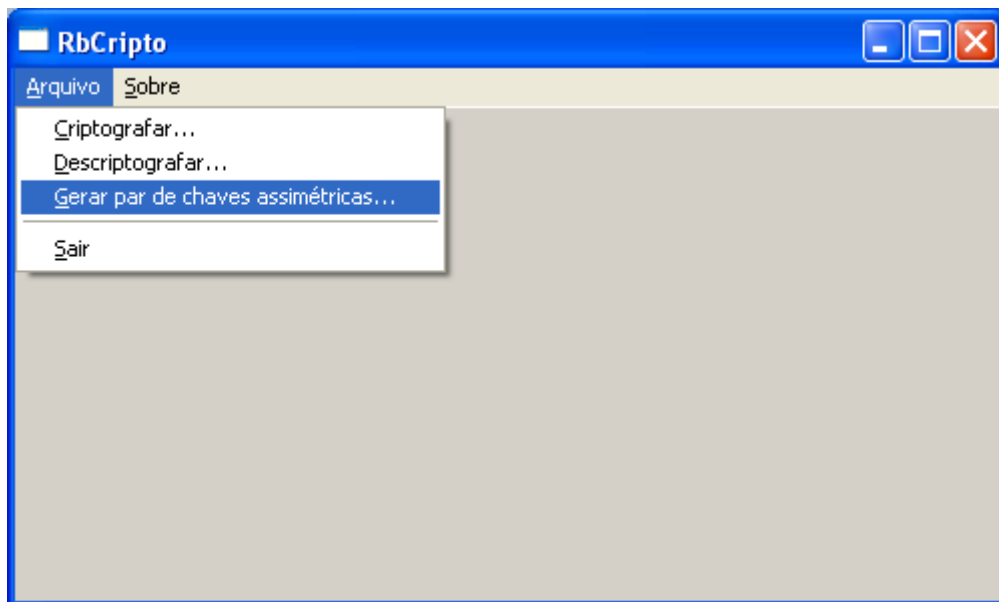
## **Criptografia assimétrica versus criptografia simétrica**

A diferença entre os dois conceitos é simples: na criptografia simétrica, a mesma chave usada para encriptar o arquivo deve ser usada para deciptá-lo; na assimétrica, as chaves são distintas e possuem uma correlação baseada em conceitos matemáticos complexos. O RbCripto suporta os dois tipos. Para usar a criptografia simétrica, o usuário deverá digitar uma senha, que será convertida em chave criptográfica para encriptar o arquivo. Para deciptá-lo, deverá lembrar a mesma senha para possibilitar o processo inverso. Para usar a criptografia assimétrica, o usuário precisará apenas gerar um par de chaves, que serão salvas em arquivos.

## **Como usar o programa**

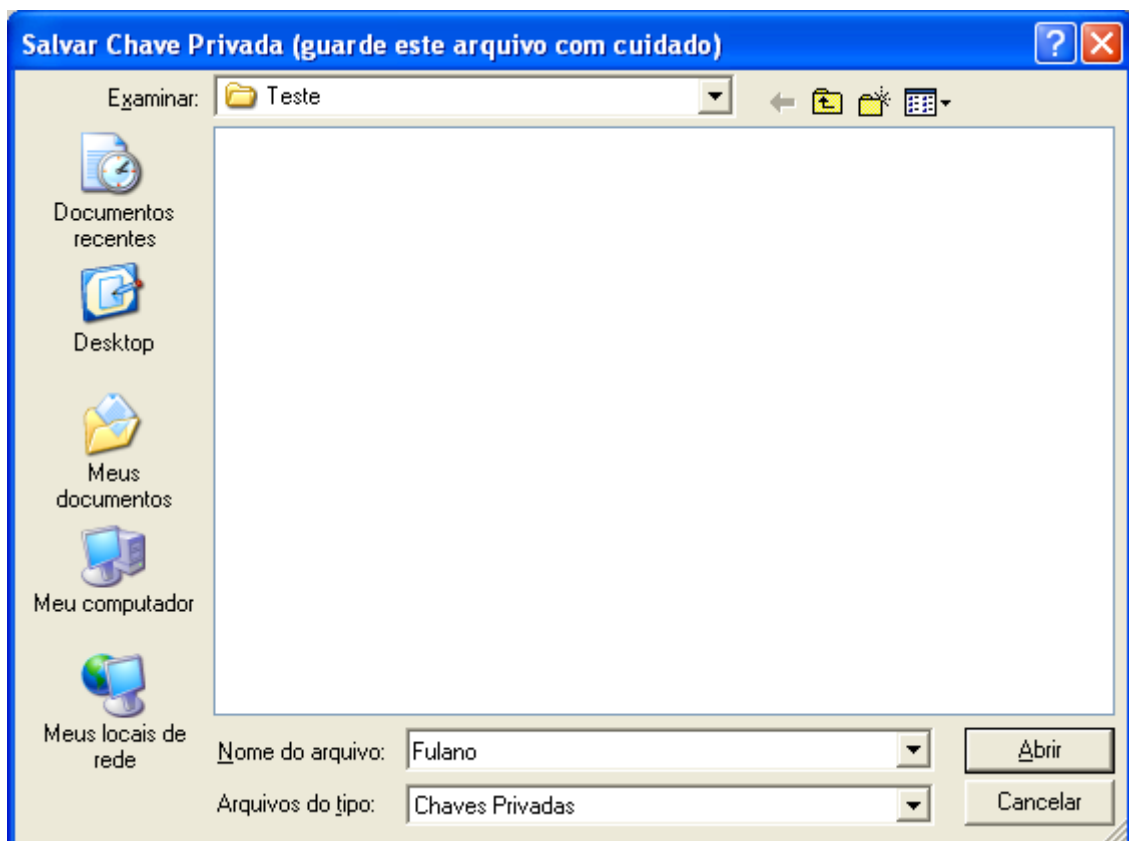
### **Geração de chaves assimétricas**

As chaves assimétricas são usadas para fazer a encriptação e deciptação do arquivo sem a necessidade de usar senhas. Funciona da seguinte forma: o usuário cria um par de chaves assimétricas no próprio RbCripto:

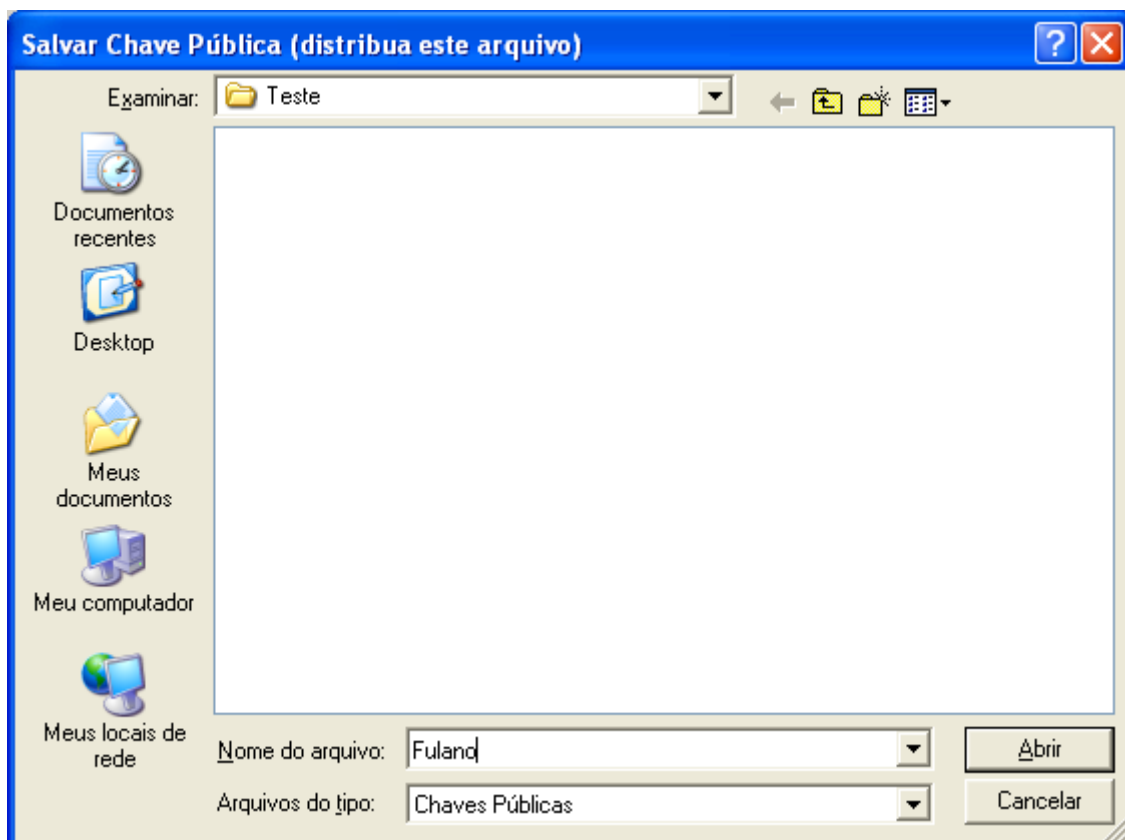


O programa gerará as chaves automaticamente e abrirá as caixas de diálogo para gravação dos arquivos.

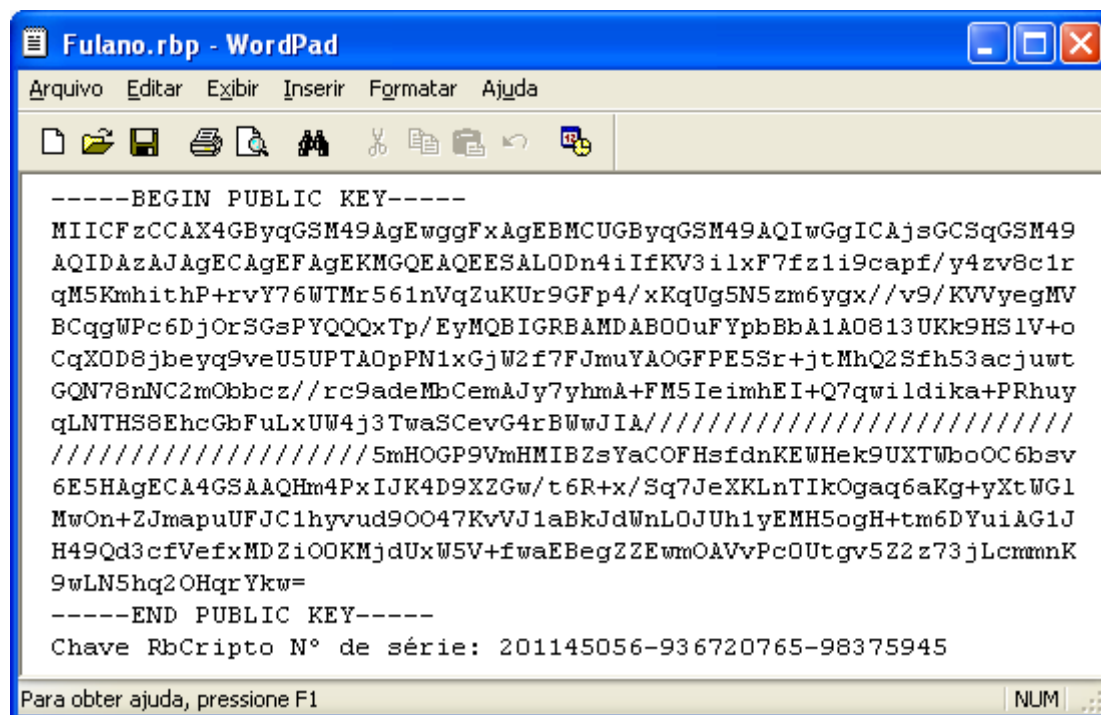
O primeiro arquivo a ser gravado é a chave privada – este arquivo deve ser armazenado com cuidado e jamais ser publicado:



O segundo arquivo é a chave pública – este arquivo deve ser distribuído e outras pessoas o usarão para encriptar arquivos que só podem ser decriptados com sua chave privada, que foi guardada com cuidado:

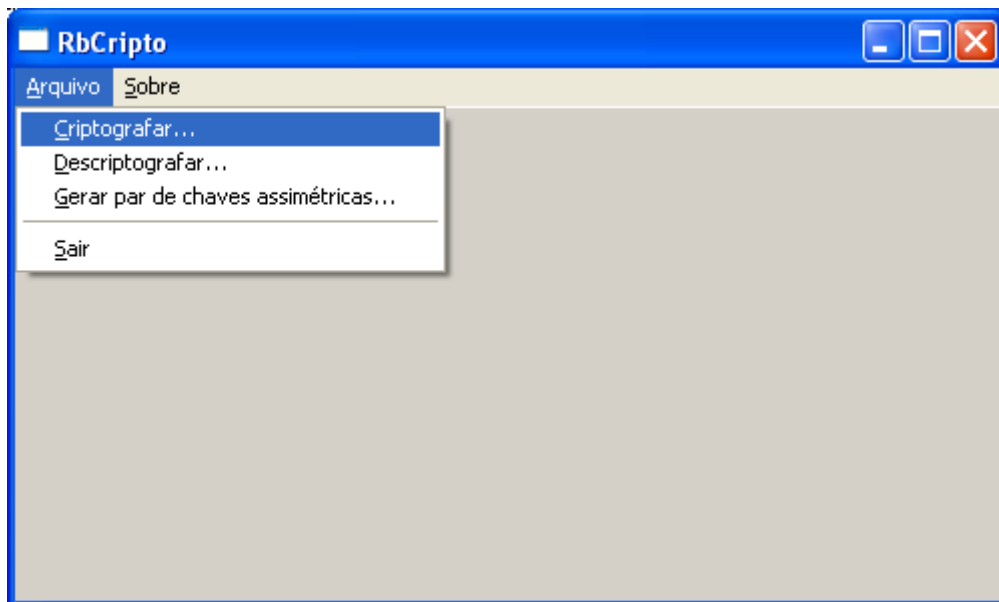


Este é o exemplo de uma chave RbCripto:

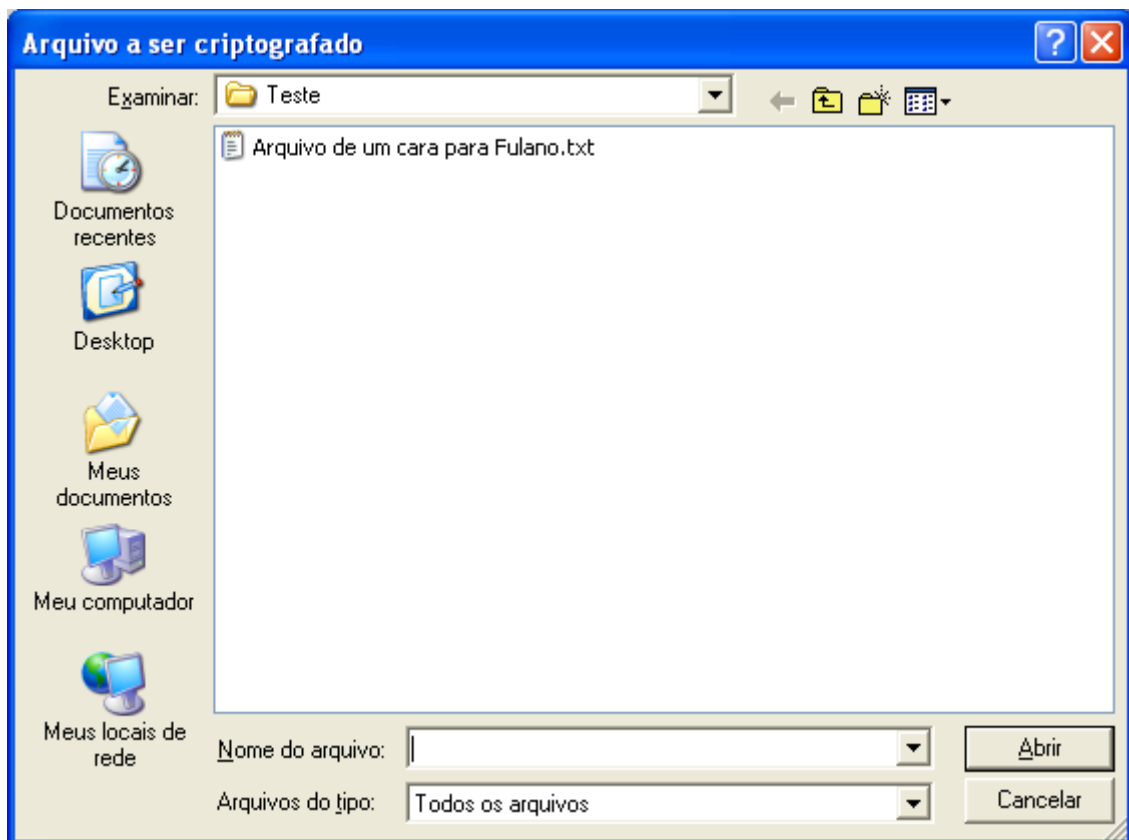


## Encriptação

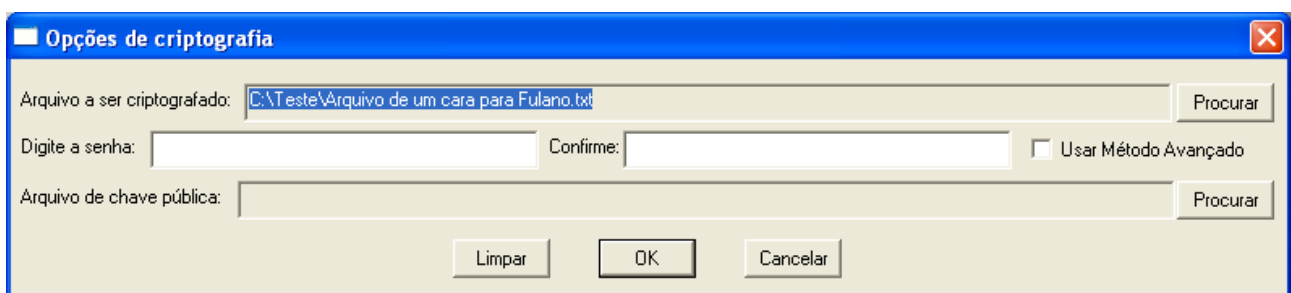
É muito simples, entre na função CRIPTOGRAFAR:



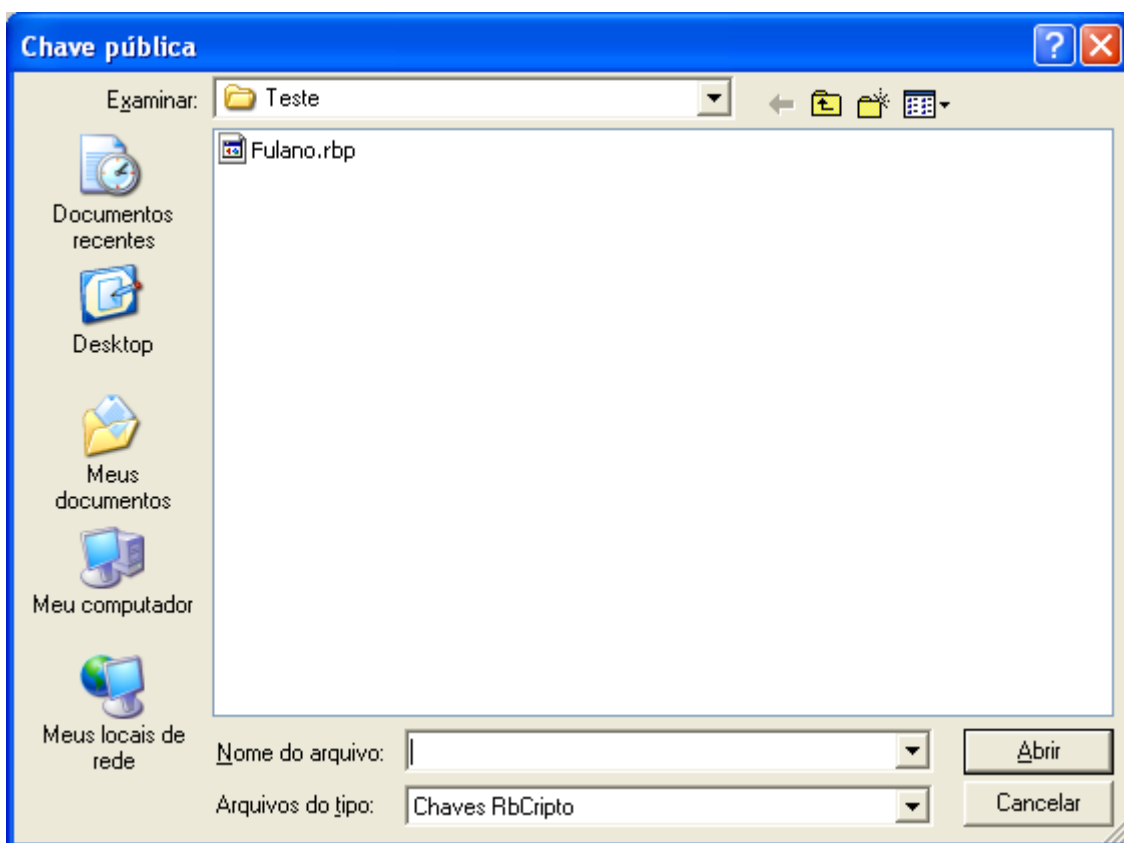
O RbCripto abrirá a caixa para escolher o arquivo a ser encriptado:



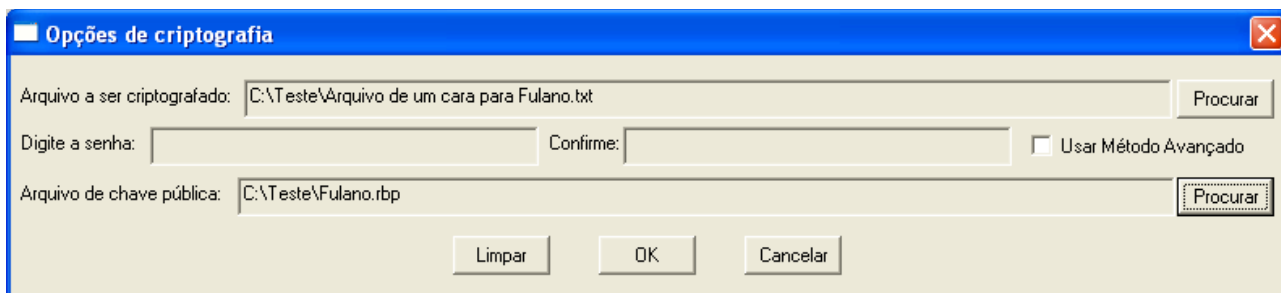
Após a escolha, abrirá uma caixa de opções como esta:



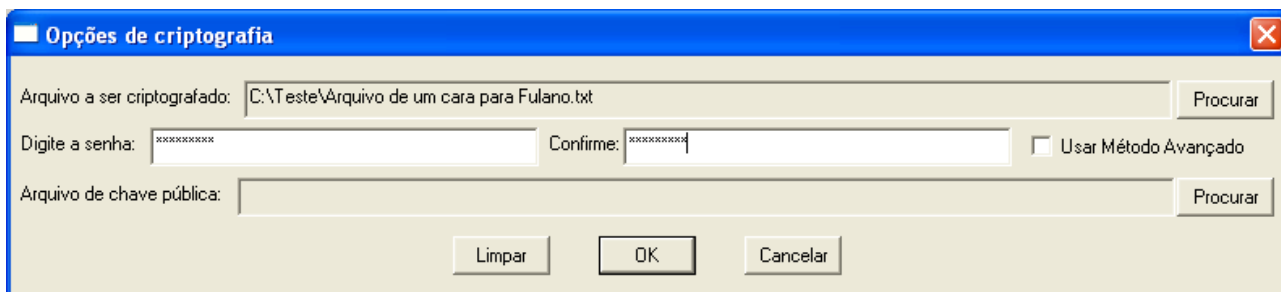
Caso queira usar a criptografia assimétrica, basta utilizar o botão PROCURAR ao lado do campo “Arquivo de chave pública” para localizar o arquivo correspondente:



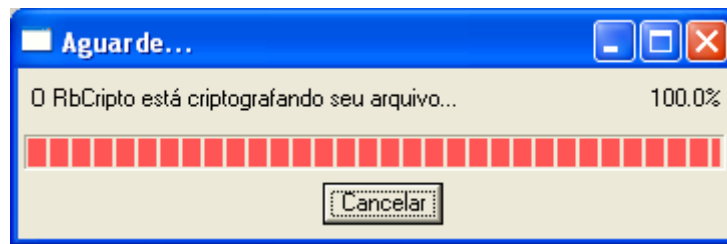
No exemplo abaixo, qualquer pessoa (ou o próprio Fulano) vai encriptar um arquivo que somente Fulano poderá decriptar, pois somente ele possui a chave privada correspondente:



Caso queira usar a criptografia simétrica, o usuário precisará digitar e confirmar uma senha:

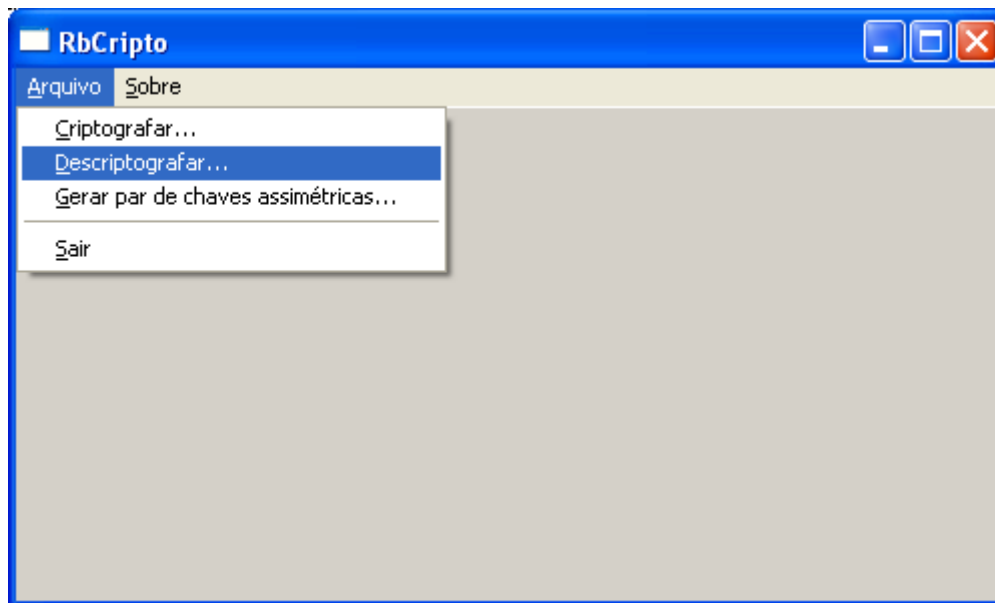


Em qualquer caso, é recomendável selecionar “Usar Método Avançado”, pois assim o RbCripto usará variações no algoritmo para deixar o arquivo mais seguro sem precisar de mais tempo para isso. Durante o processamento, o RbCripto exibirá uma barra de progresso como esta:

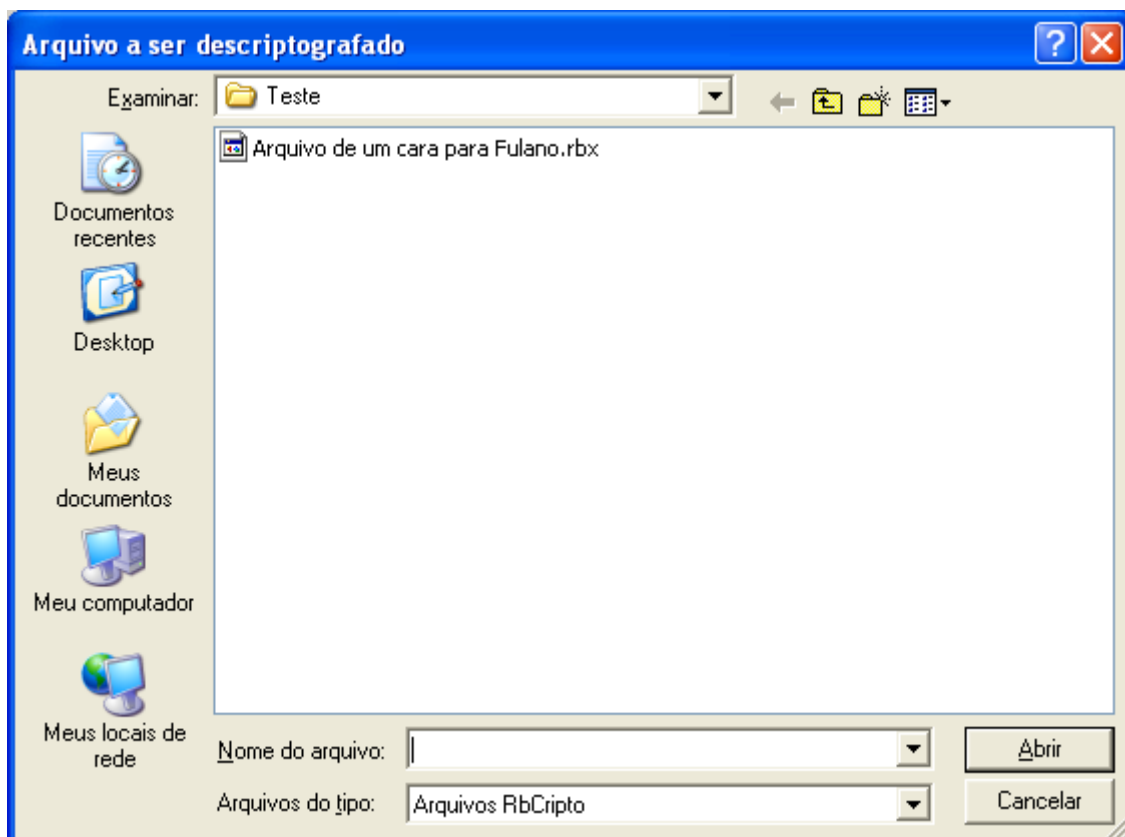


## Decriptação

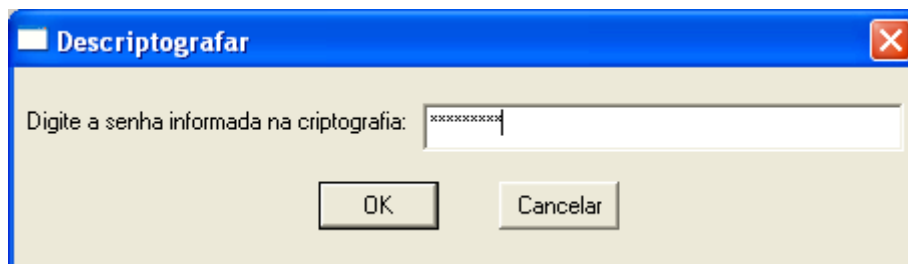
Para decriptar um arquivo, o processo é ainda mais simples. Escolha a função DESCRIPTOGRAFAR:



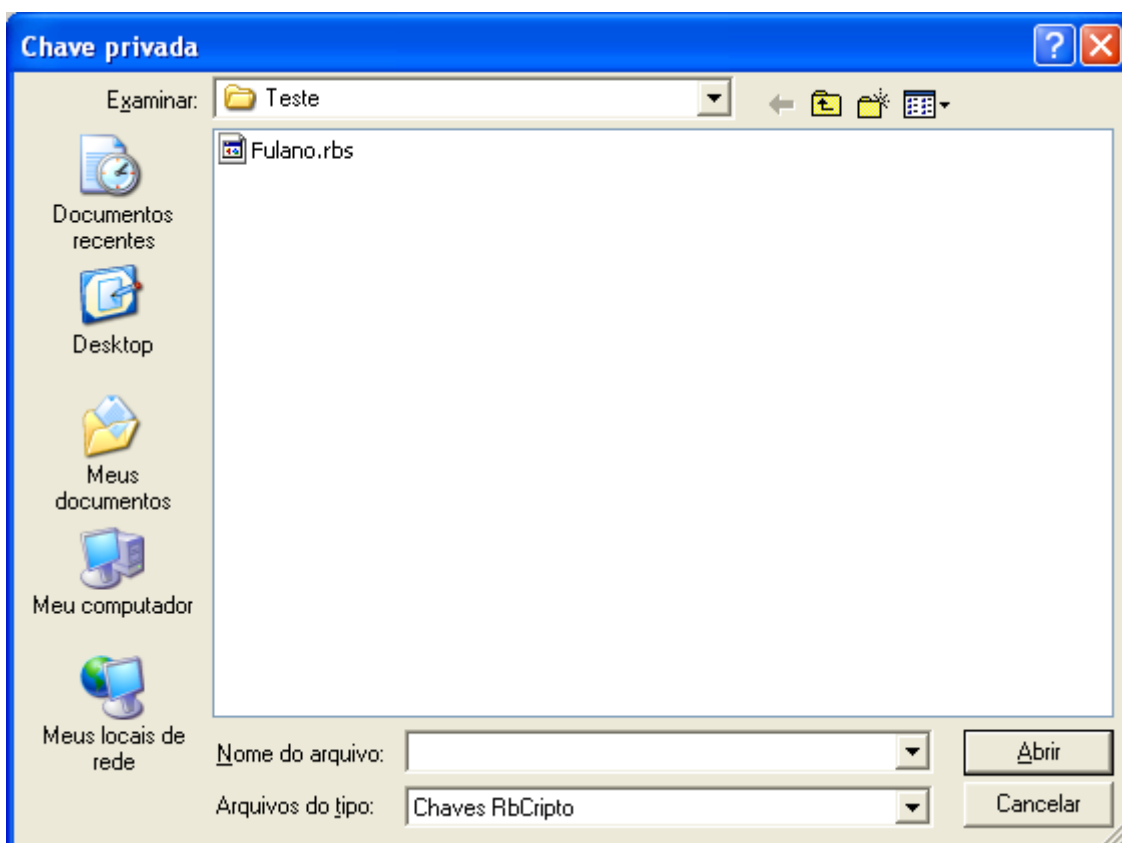
Selecione o arquivo a ser decriptado:



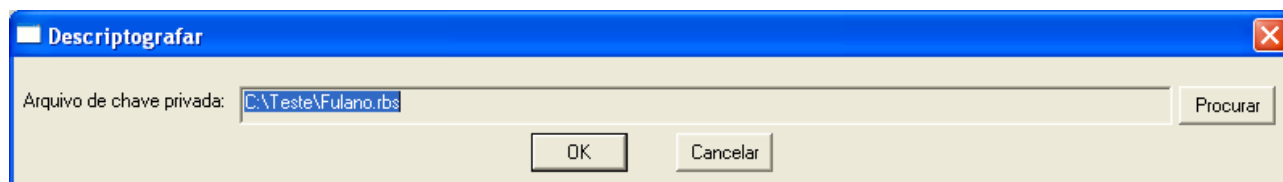
O RbCripto detectará automaticamente as opções usadas na encriptação e agirá de acordo. Caso tenha sido usada a criptografia simétrica, pedirá uma senha em uma caixa como esta, na qual o usuário deverá digitar a mesma senha usada para encriptar:



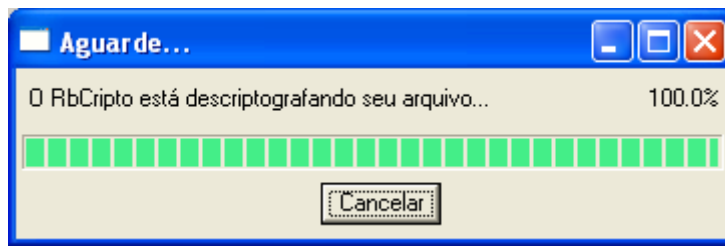
Caso o usuário tenha optado pela criptografia assimétrica, o RbCripto precisará do arquivo de chave privada correspondente ao arquivo de chave pública usado para encriptar. Por exemplo, se alguém ou o próprio Fulano usou a chave pública de Fulano para encriptar, o programa precisará da chave privada de Fulano (que só ele possui) e pedirá o arquivo que possui esta chave. Quando abrir a caixa, basta selecionar o arquivo correto:



E o arquivo poderá ser decriptado normalmente:



Durante o processamento, o RbCripto exibirá uma barra de progresso como esta:



### ***Avançado – envio de chaves públicas por e-mail***

Para a criptografia assimétrica, é necessário distribuir a chave pública. É claro que enviar por e-mail é a primeira ideia para fazer a distribuição. Como muitos provedores de e-mail bloqueiam arquivos anexos hoje em dia, anexar o arquivo de chave pública (extensão RBP) pode dar problema. Mas há uma maneira de contornar isso: basta abrir o arquivo com o Wordpad, por exemplo, copiar seu conteúdo e colar no corpo da mensagem. A única restrição é que a mensagem não pode ter formatação HTML (qualquer programa de e-mail ou interface *webmail* na Internet permite esta opção). A pessoa que receber o e-mail simplesmente precisa colar o texto na janela do Wordpad e salvar o arquivo com a extensão RBP.