👥 Autores

- KAUA MACHADO DA SILVA
- ALAN NUNES VELOSO NOGUEIRA
- MATHEUS KAIKY BRITO SILVA

Projeto: Envelope Digital com Criptografia RSA + AES

Este projeto é uma aplicação para criação e abertura de envelopes digitais, combinando criptografia RSA e AES com diferentes modos e for

📁 Estrutura do Projeto

```
Envelope_Digital/
│
├── 📂 assets/                # Recursos não-código
│   ├── 📂 images/            # Capturas de tela e imagens da interface
│   └── 📂 diagrams/          # Diagramas de arquitetura e fluxo
│
├── 📂 src/                   # Código-fonte principal
│   ├── 📜 utils.py           # Utilitários: padding PKCS7, codificação
Base64Hex
│   ├── 🔐 rsa_manager.py     # Gera e carrega chaves RSA (1024/2048 bits)
│   ├── 🔒 aes_manager.py    # Implementa AES (128/192/256 bits) nos modos
ECB/CBC
│   ├── ✉️ envelope.py        # Combina RSA+AES para criar/abrir envelopes
digitais
│   ├── 🚀 app.py             # Ponto de entrada do aplicativo
│   └── 🔌 main.py
├──
├── 📜 requirements.txt       # Dependências: cryptography, tkinter, etc.
├── 📜 README.md              # Documentação completa
│
├── 📂 teste/                 # Arquivos gerados automaticamente
│   ├── 🔑 chaves_rsa/        # Armazena chaves públicas/privadas (.pem)
│   ├── 📄 mensagens/         # Mensagens criptografadas/descriptografadas
│   └── 🔐 chaves_aes/        # Chaves AES criptografadas
```

🚀 Funcionalidades

- 🔐 **Geração de chaves RSA** (1024 ou 2048 bits) para criptografia assimétrica.
- ✉️ **Criação de envelope digital** utilizando criptografia híbrida (RSA para a chave AES e AES para a mensagem).

- 📂 **Abertura de envelope digital**, permitindo a descriptografia da mensagem e da chave AES utilizando a chave privada RSA.
- 🧾 **Codificação em Base64 ou Hexadecimal** para facilitar a leitura e escrita dos arquivos criptografados.
- 🔄 **Modos de operação AES**:
  - **ECB** (Electronic Codebook) para operações sem IV.
  - **CBC** (Cipher Block Chaining) com **IV** (vetor de inicialização) para maior segurança na criptografia.
- 🎛️ **Interface gráfica (GUI)** utilizando Tkinter, com funcionalidades de rolagem para visualizar o conteúdo de arquivos criptografados e descriptografados.
- 📁 **Armazenamento automático** dos arquivos de chave, mensagem criptografada e IV (se necessário) em uma pasta `teste/`, para facilitar o gerenciamento de dados durante os testes.

🛠️ Instalação e Configuração do Ambiente

1. **Instale e selecione a versão do Python**

   → **Versão do Python utilizada:** 3.13.3

2. **Instale as dependências necessárias:**

   ```
   pip install -r requirements.txt
   ```

   → Instale todas as dependências do projeto listadas no arquivo `requirements.txt`.

▶ Como Usar

1. 💻 **Inicie o aplicativo:**

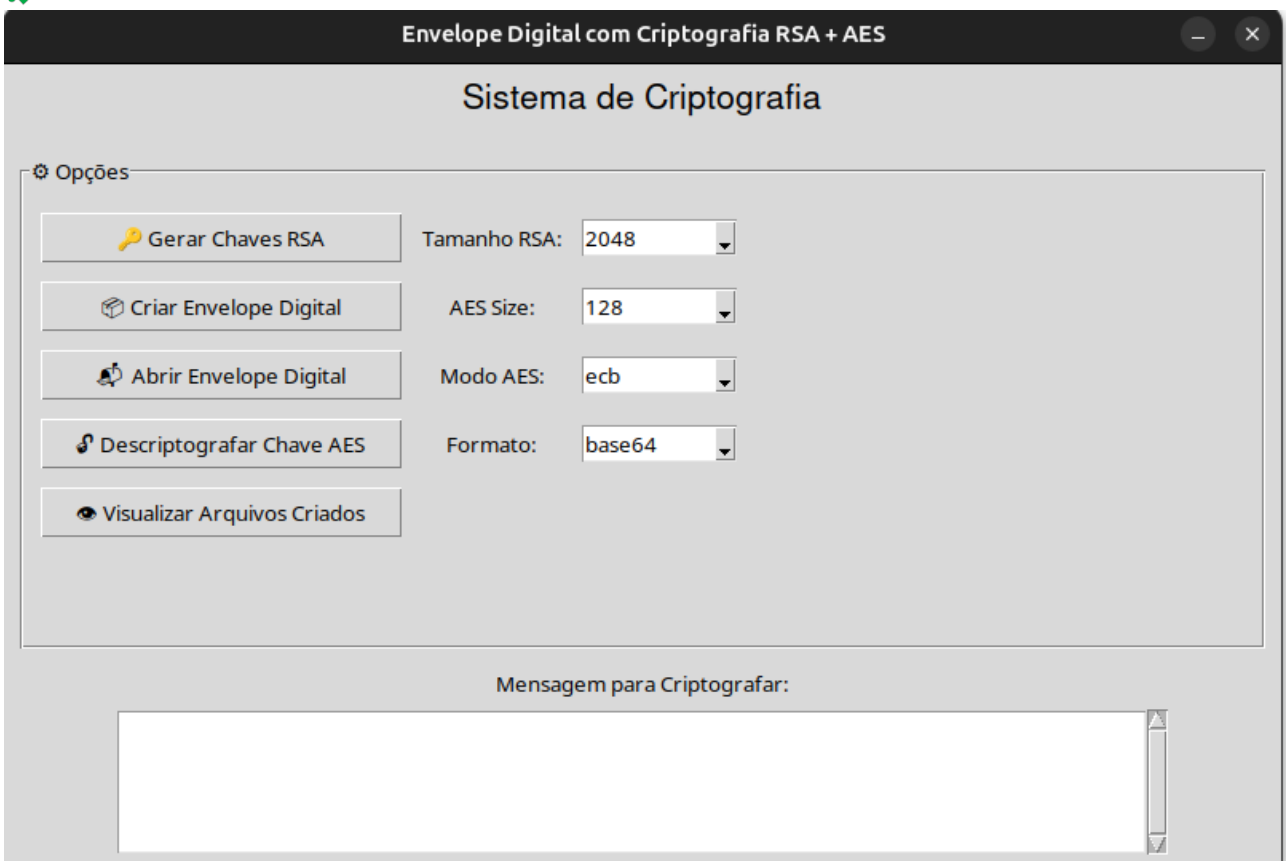
   Abra o terminal e execute o seguinte comando para iniciar a interface gráfica:

   ```
   python3 src/app.py #Windows python src/app.py
   ```

   Isso iniciará o aplicativo e abrirá a interface gráfica, permitindo que você utilize todas as funcionalidades.

---

2. 🧩 **Recursos da Interface**



A interface gráfica permite interagir com as principais funcionalidades do aplicativo. Alguns recursos incluem:

- **Geração de Chaves RSA:**
  - Selecione o tamanho da chave (1024 ou 2048 bits) para criar um par de chaves RSA (pública e privada).
- **Criação de Envelope Digital:**
  - Insira uma mensagem para criptografá-la utilizando a criptografia híbrida (RSA + AES).
  - A chave AES será gerada e criptografada com a chave pública RSA.
- **Abertura de Envelope Digital:**
  - Selecione um arquivo de envelope digital criptografado.
  - Descriptografe a chave AES com a chave privada RSA e depois a mensagem criptografada.
- **Codificação Base64 ou Hexadecimal:**
  - Escolha o formato de codificação para visualizar a chave ou a mensagem criptografada.
- **Modos de Operação AES:**
  - Selecione entre os modos de operação ECB ou CBC (com IV) para a criptografia AES.
- **Exibição de Arquivos:**
  - A interface possui uma área de rolagem para permitir a visualização dos arquivos Gerados

Esses recursos são acessíveis diretamente na interface, facilitando o uso das funcionalidades do aplicativo.

📖 Exemplos Práticos

🔑 Exemplo 1: Gerar Chaves RSA

Objetivo: Criar um par de chaves pública/privada para criptografia assimétrica.

```
Escolha: 🔑 Gerar Chaves RSA
Tamanho da chave RSA: (1024/2048): 2048
Digite o nome da chave pública: public.pem
Digite o nome da chave privada: private.pem

📂 Arquivos gerados:
teste/
├── public.pem    # Chave pública (compartilhável)
└── private.pem   # Chave privada (sigilosa)
```

✉️ Exemplo 2: Criar Envelope Digital

```
Caixa Digite a Mensagem: ''Dados confidenciais 123@!''
Tamanho AES: 256
Modo: cbc
Formato: hexadecimal
Escolha: 📦 Criar Envelope Digital
Chave pública: public.pem
Digite o nome Arquivo chave cifrada: encrypted_key
Digite o nome Arquivo mensagem cifrada: encrypted_msg
Digite o nome Arquivo IV: iv

📂 Arquivos gerados:

teste/
├── encrypted_key.txt
├── encrypted_msg.txt
└── iv.txt
```

🔓 Exemplo 3: Abrir Envelope Digital

```
Modo: cbc
Formato: hexadecimal
Escolha: 📬  Abrir Envelope Digital
Mensagem cifrada: encrypted_msg
Arquivo Chave cifrada: encrypted_key
Arquivo Chave privada: private.pem
```

```
Arquivo IV: iv.b64
Digite o nome Arquivo Saída: decrypted.txt

📂 Arquivos gerados:

teste/
└── idecrypted.txt
```

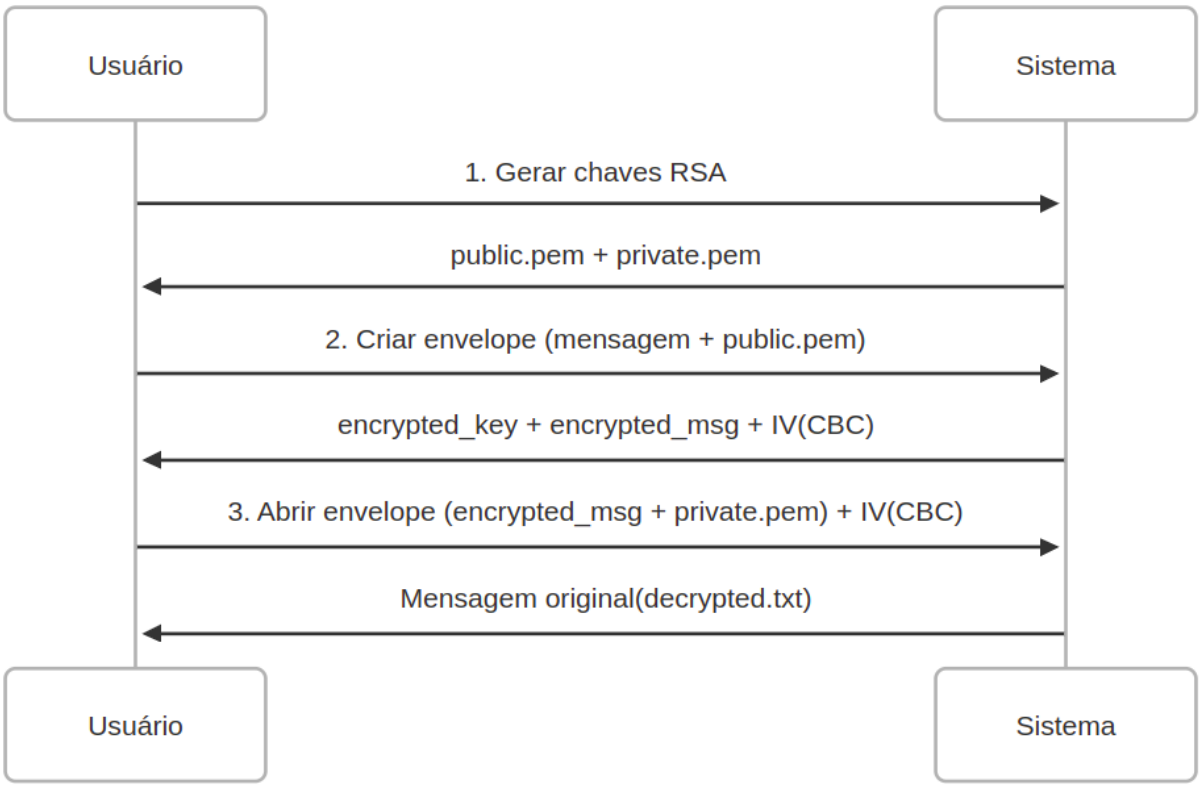
🔓 Exemplo 4: Descriptografar Chave AES

```
Escolha: 🔓 Descriptografar Chave AES
Arquivo Chave cifrada: encrypted_key
Arquivo Chave privada: private.pem

📂 Arquivos gerados:

teste/
└── aes_key_decifrada.txt
```

👁️Exemplo 5: Visualizar Arquivos Criados

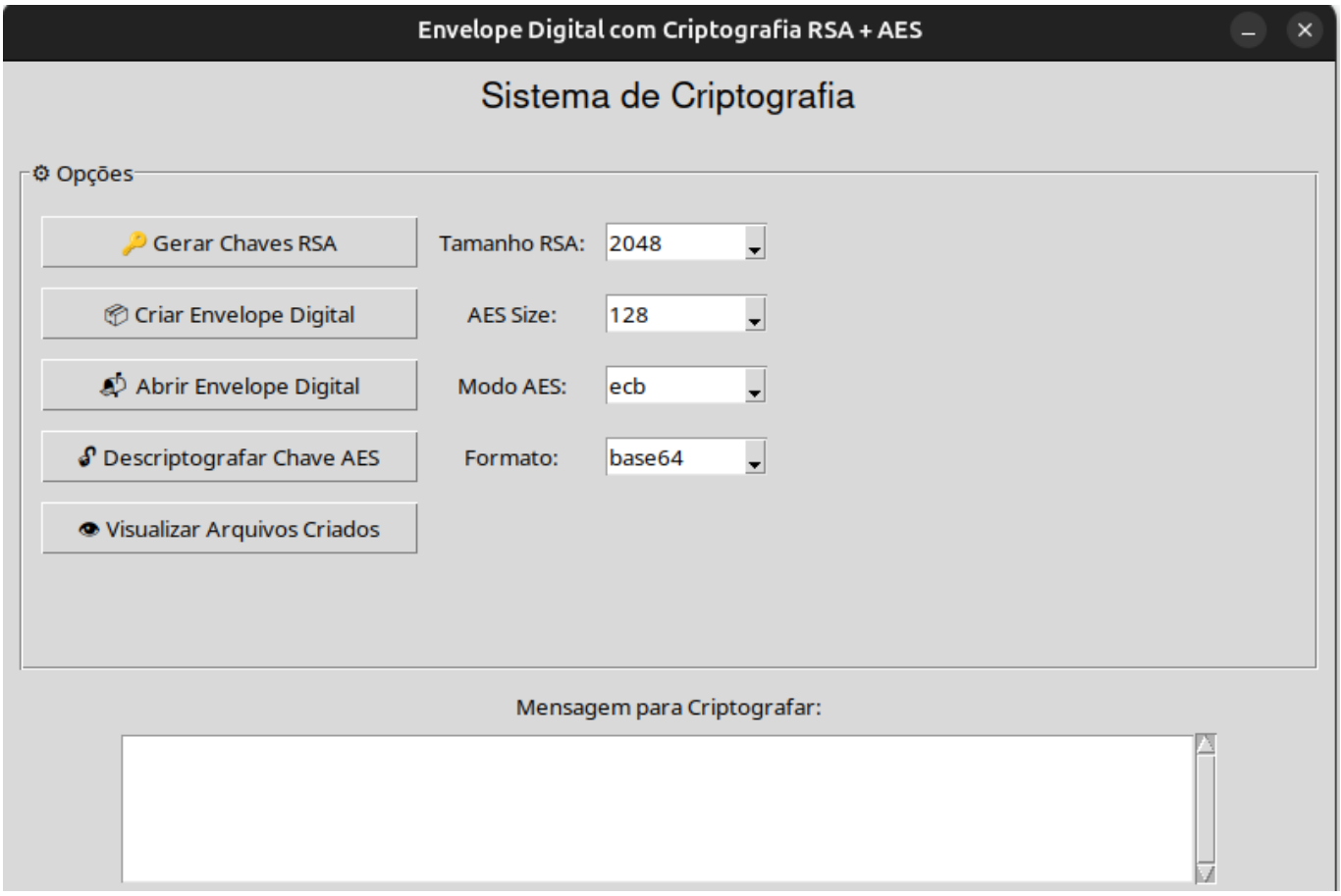
```
Escolha: 👁 Visualizar Arquivos Criados

📂 Saida:

└──  Visualização dos arquivos Gerados
```

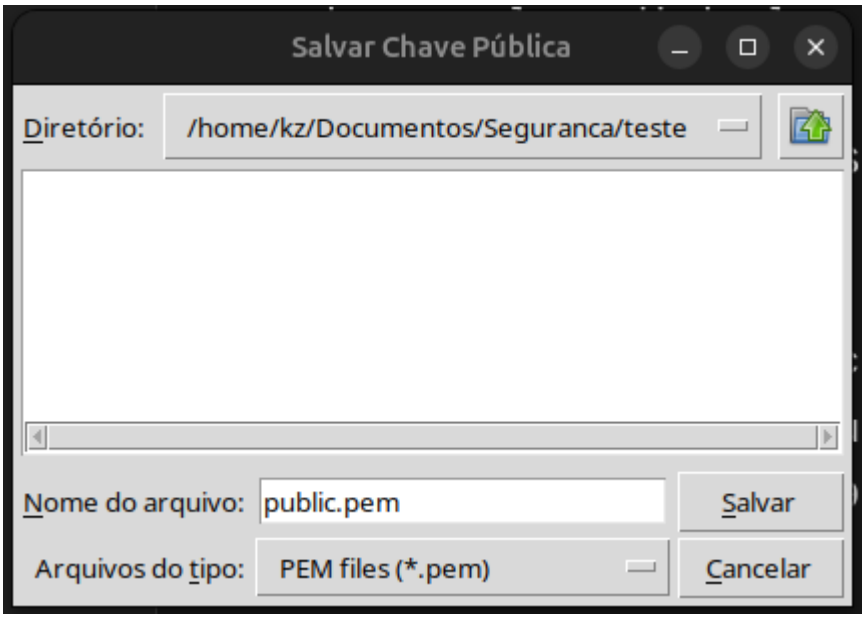
🔄 Diagrama de Fluxo

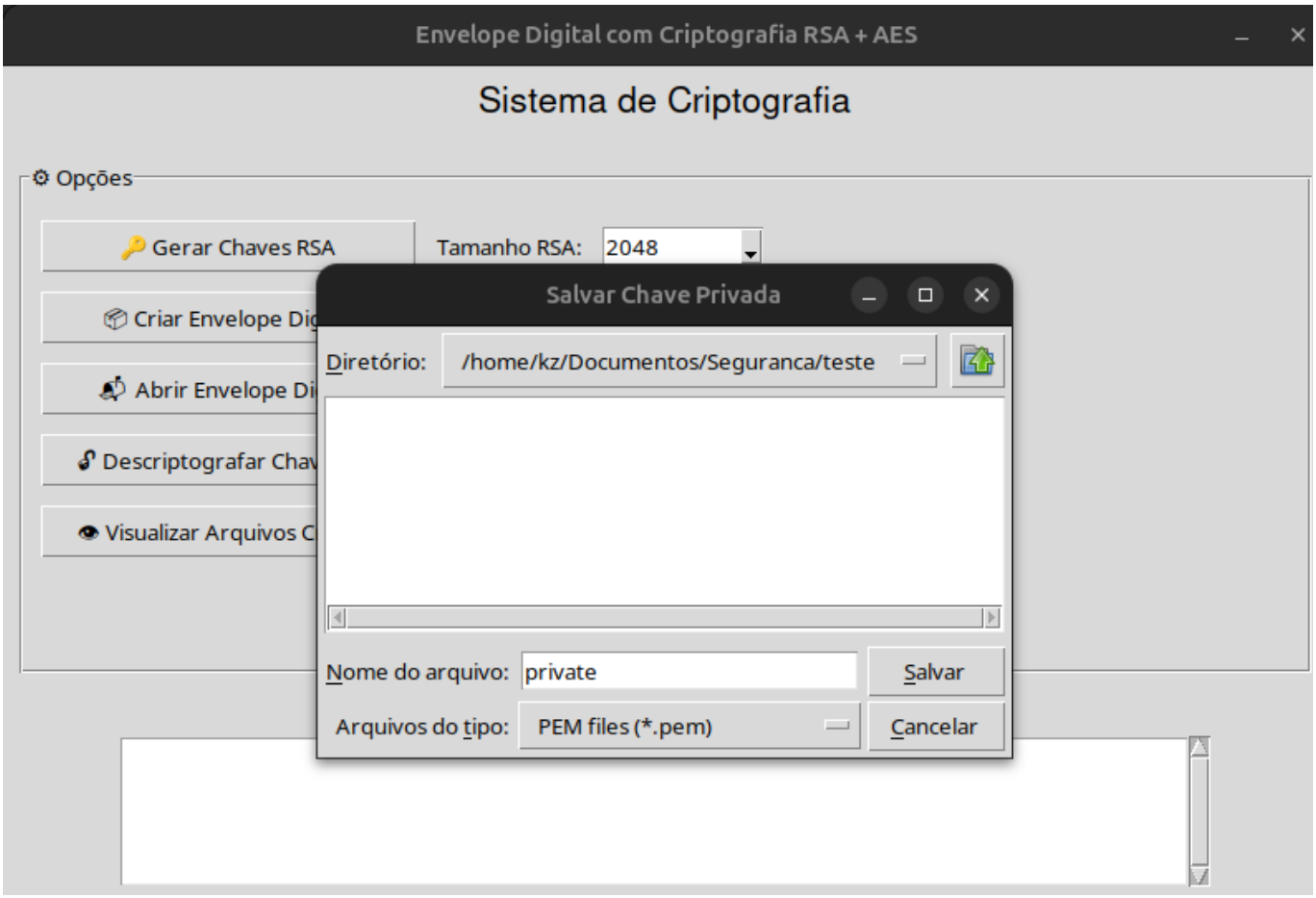


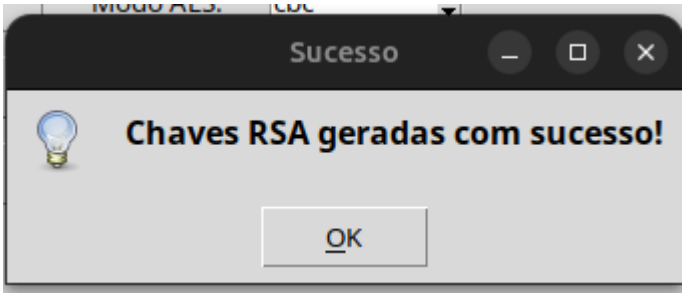
📸 Capturas de Tela

🔑 Geração de Chaves RSA

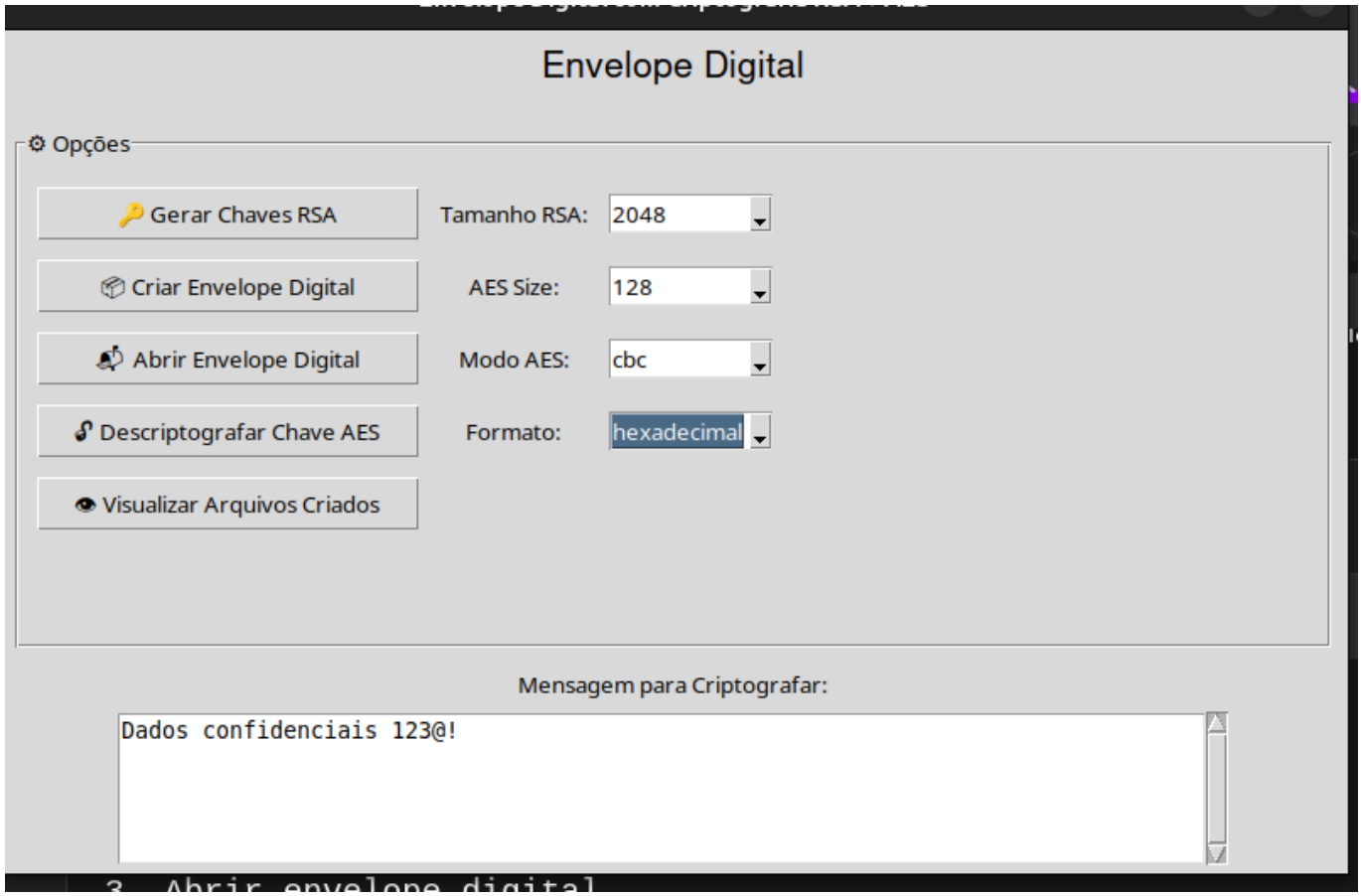

Envelope Digital com Criptografia RSA + AES
Sistema de Criptografia
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Criar Envelope Digital
AES Size:
128
Abrir Envelope Digital
Modo AES:
ecb
Descriptografar Chave AES
Formato:
base64
Visualizar Arquivos Criados
Mensagem para Criptografar:

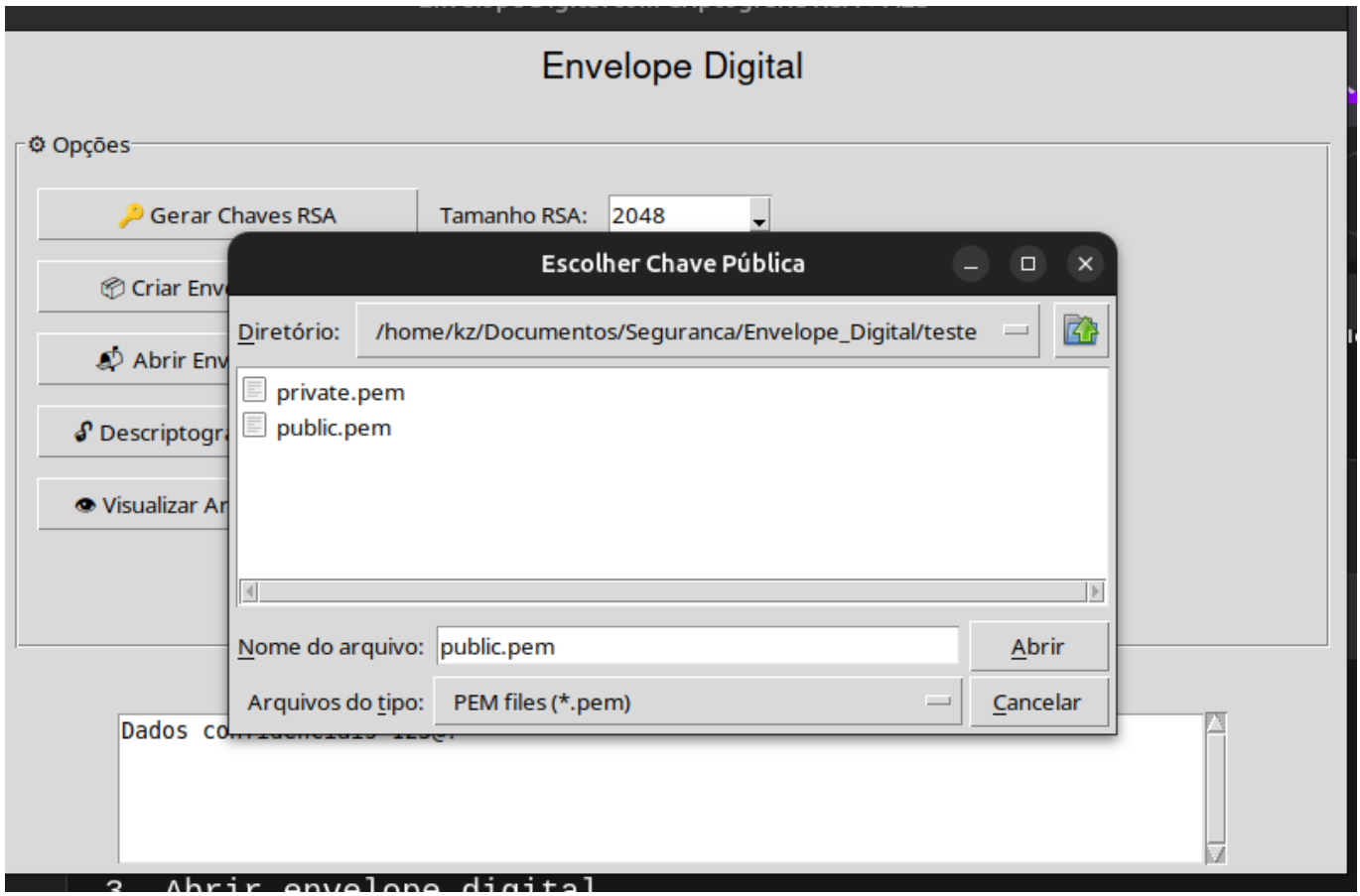

Salvar Chave Pública
Diretório:
/home/kz/Documentos/Seguranca/teste
Nome do arquivo:
public.pem
Salvar
Arquivos do tipo:
PEM files (*.pem)
Cancelar

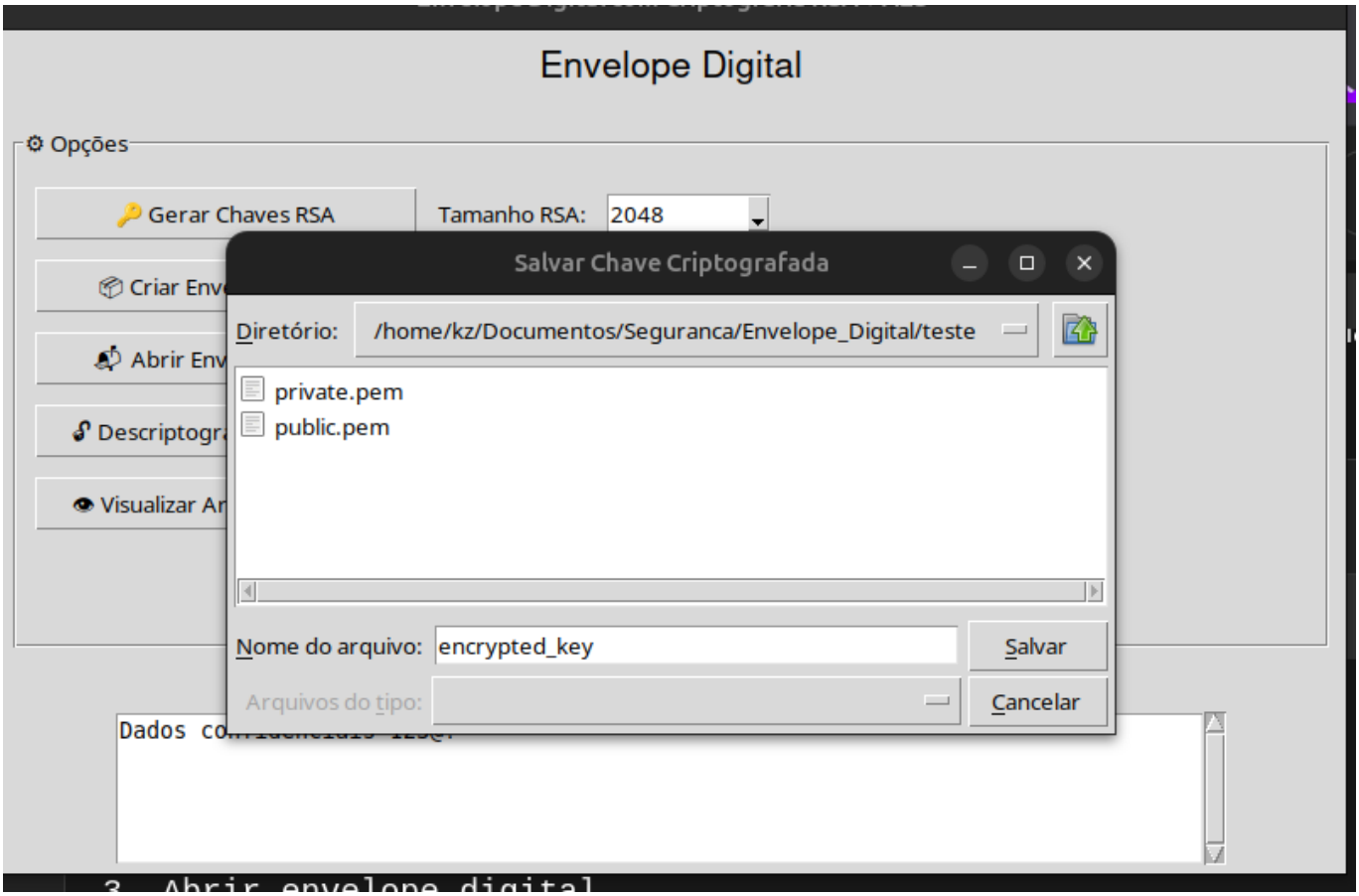


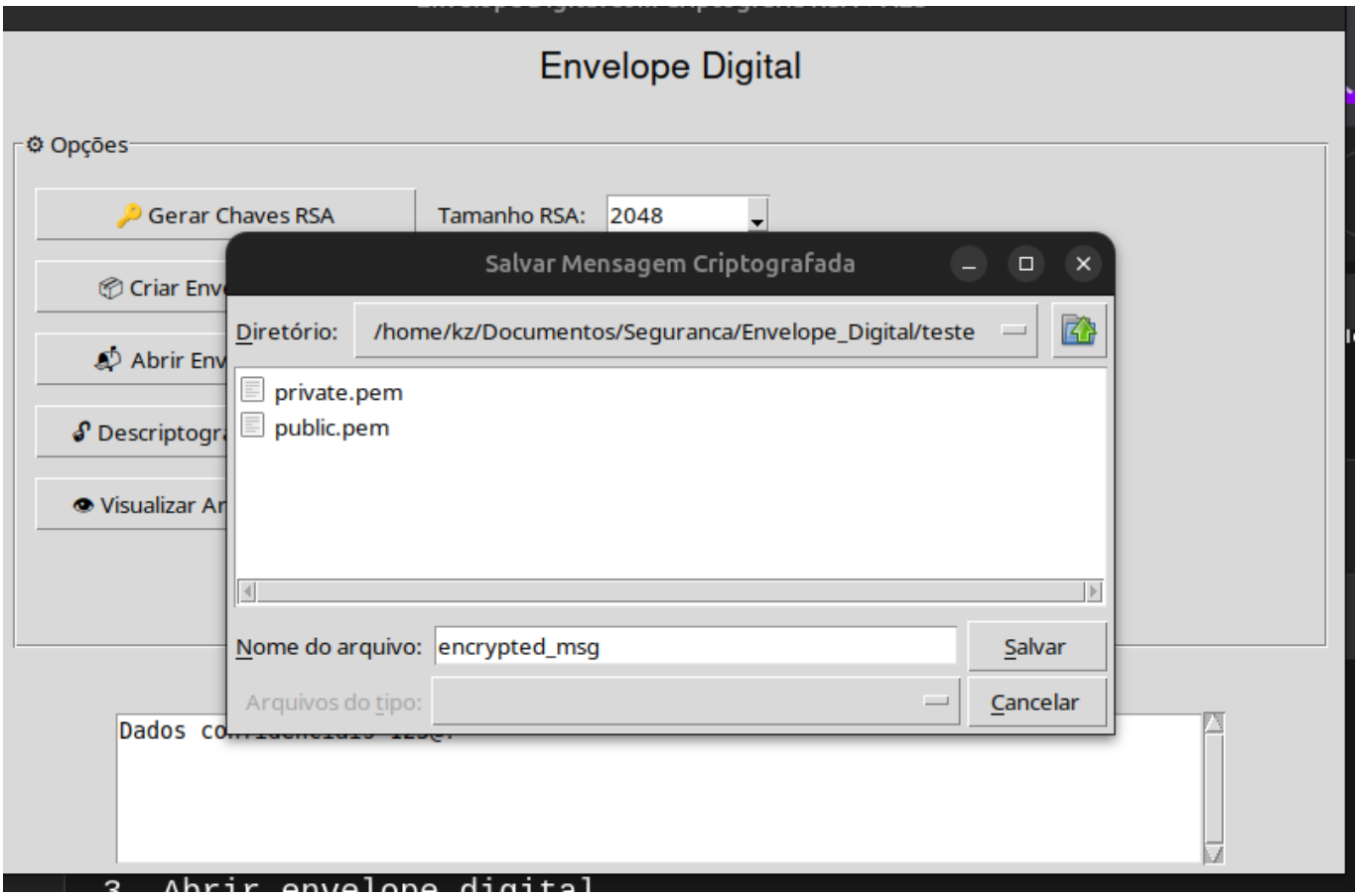


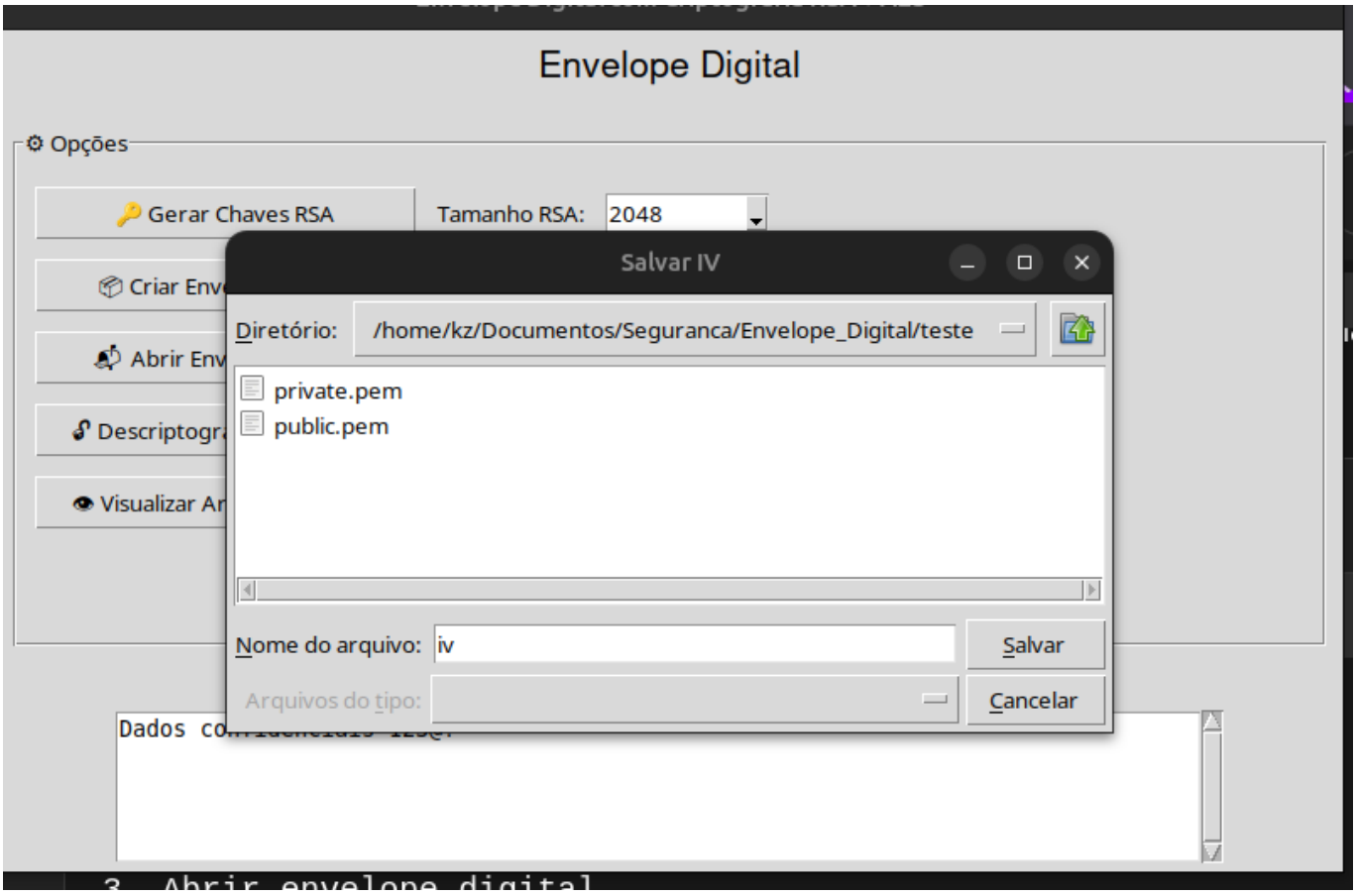
✉ Criação de Envelope


Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Criar Envelope Digital
AES Size:
128
Abrir Envelope Digital
Modo AES:
cbc
Descriptografar Chave AES
Formato:
hexadecimal
Visualizar Arquivos Criados
Mensagem para Criptografar:
Dados confidenciais 123@!

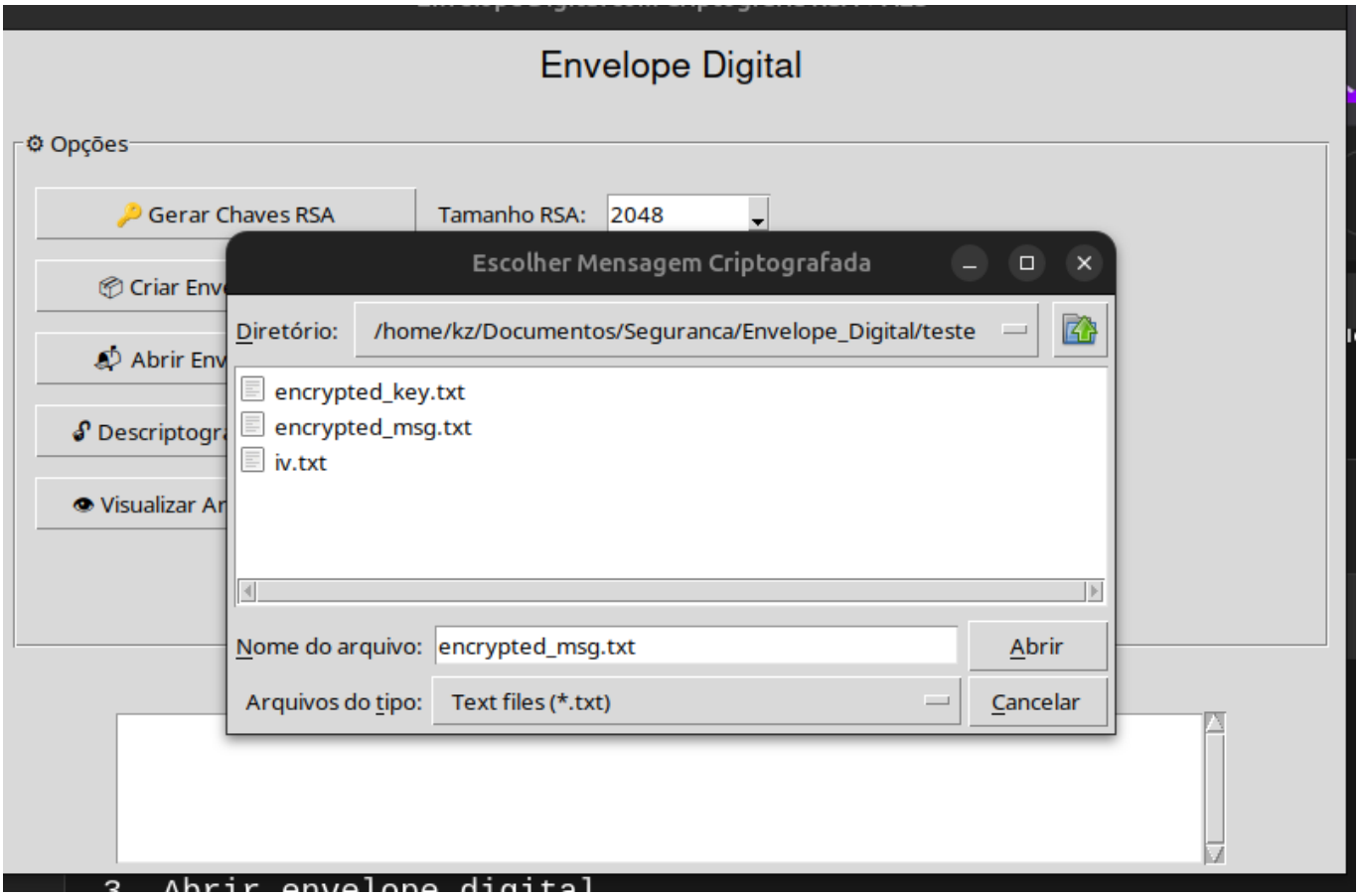

Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Escolher Chave Pública
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
private.pem
public.pem
Nome do arquivo:
public.pem
Abrir
Arquivos do tipo:
PEM files (*.pem)
Cancelar

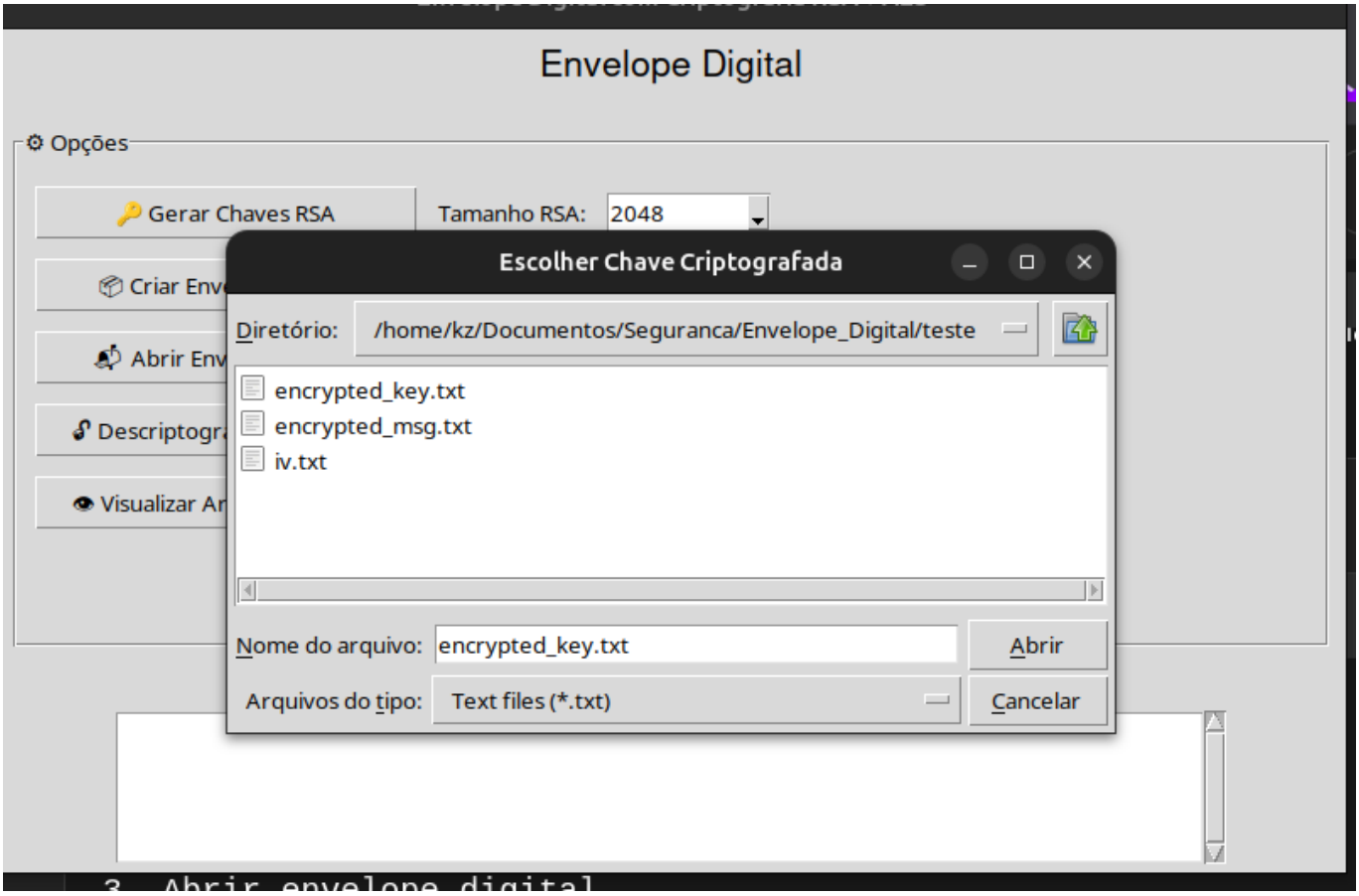

Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Salvar Chave Criptografada
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
private.pem
public.pem
Nome do arquivo:
encrypted_key
Salvar
Arquivos do tipo:
Cancelar

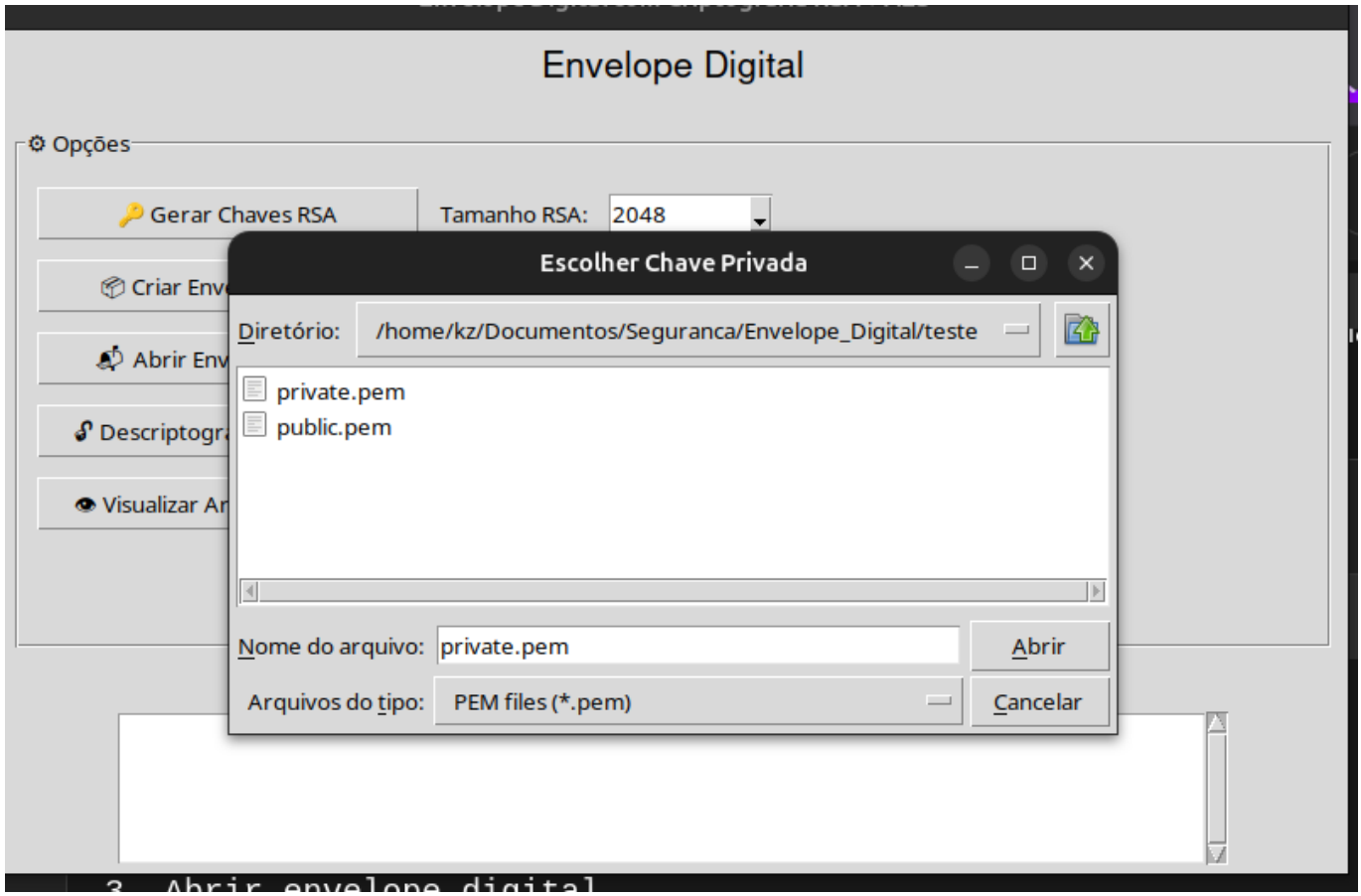

Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Salvar Mensagem Criptografada
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
private.pem
public.pem
Nome do arquivo:
encrypted_msg
Salvar
Arquivos do tipo:
Cancelar

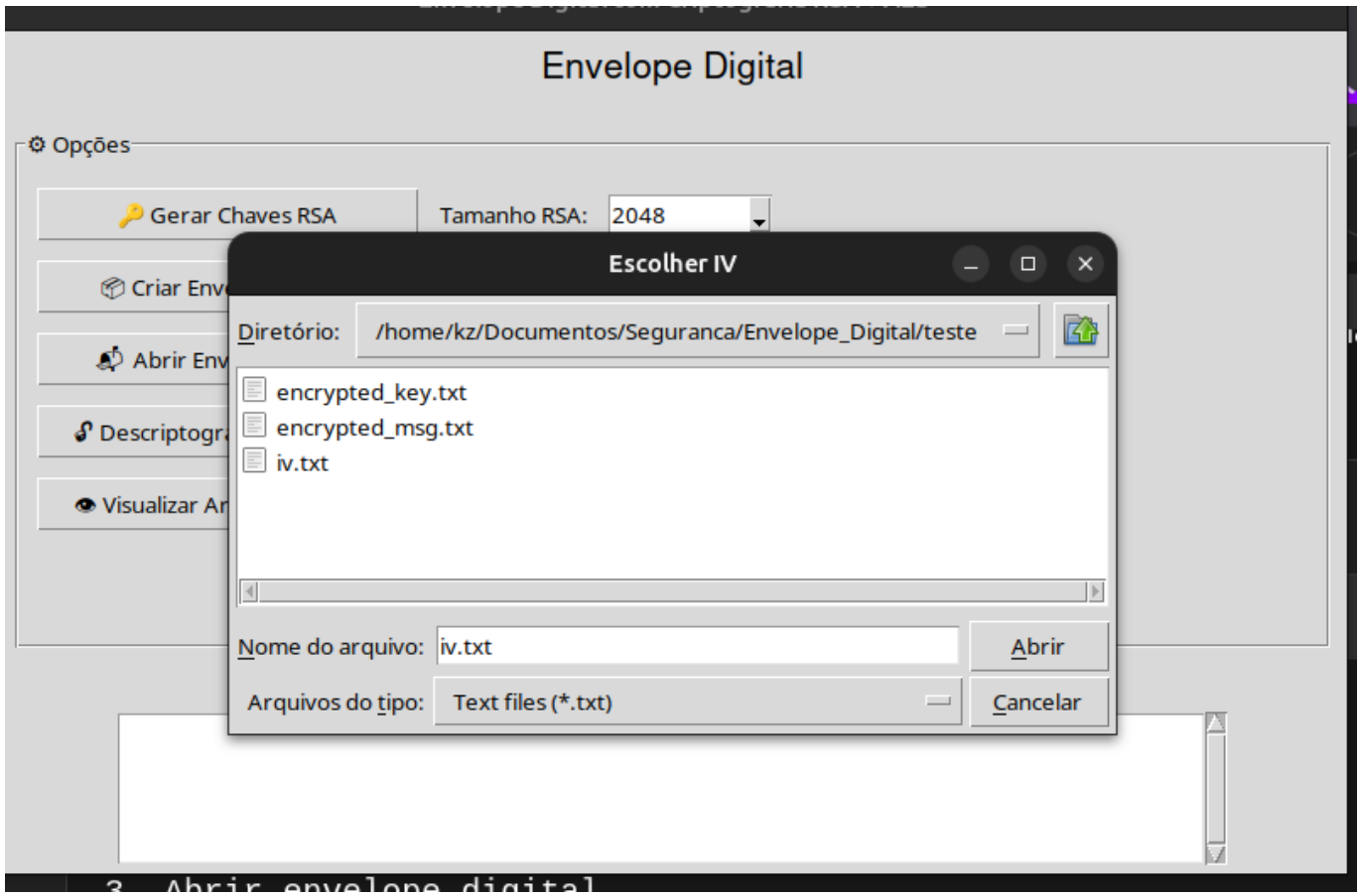


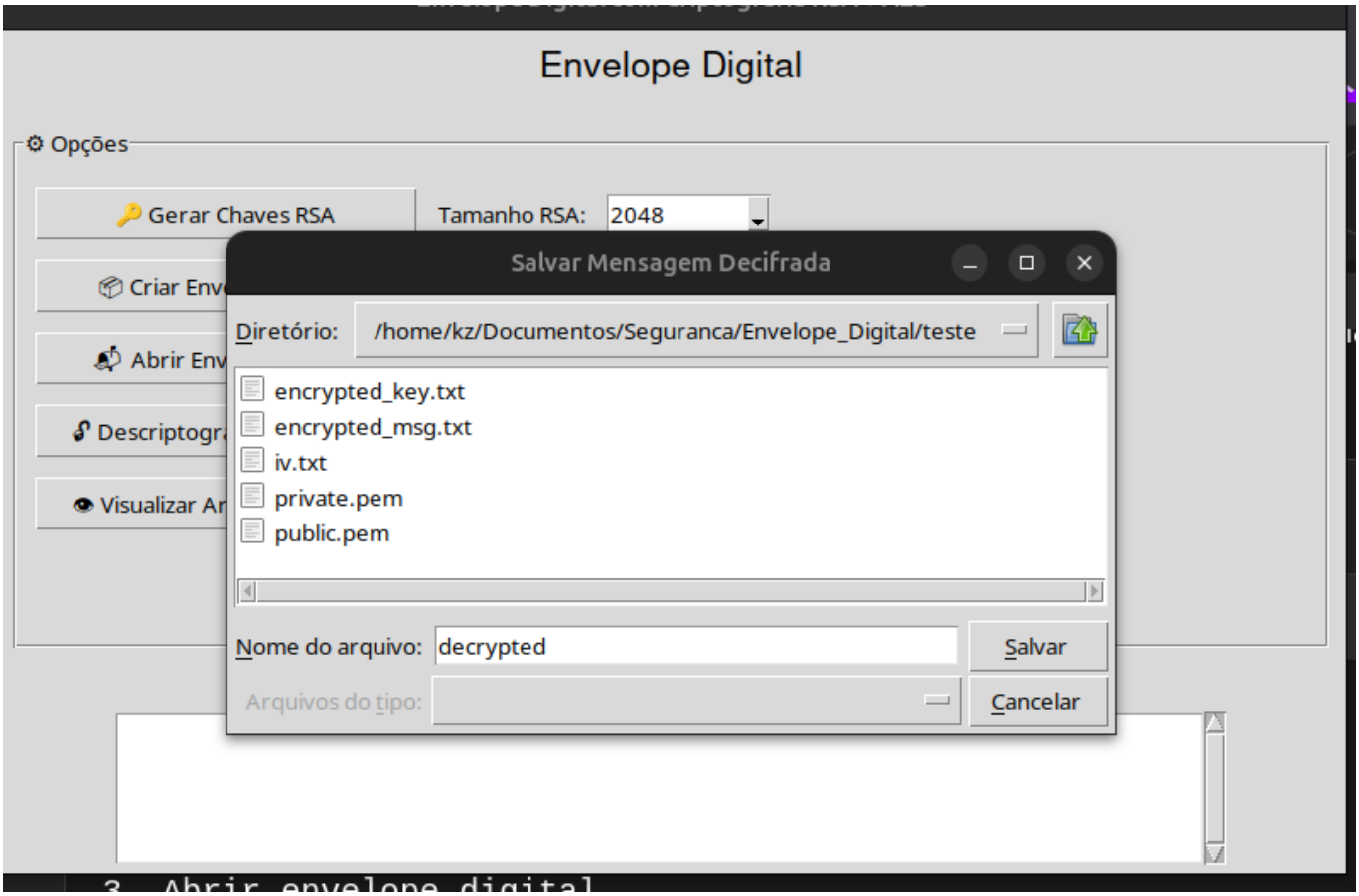
🔓 Abertura de Envelope

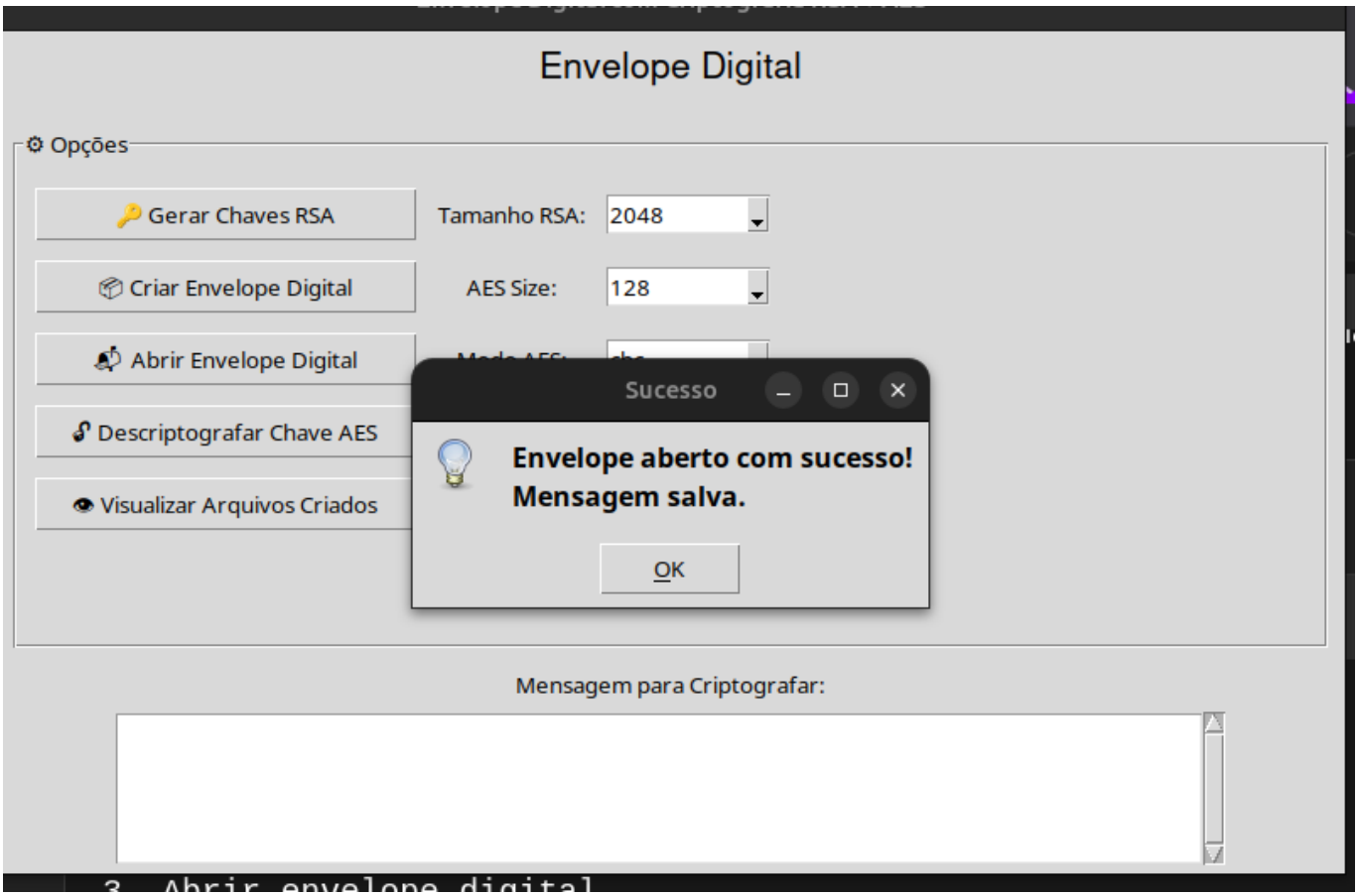

Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Escolher Mensagem Criptografada
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
encrypted_key.txt
encrypted_msg.txt
iv.txt
Nome do arquivo:
encrypted_msg.txt
Abrir
Arquivos do tipo:
Text files (*.txt)
Cancelar


Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Escolher Chave Criptografada
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
encrypted_key.txt
encrypted_msg.txt
iv.txt
Nome do arquivo:
encrypted_key.txt
Abrir
Arquivos do tipo:
Text files (*.txt)
Cancelar

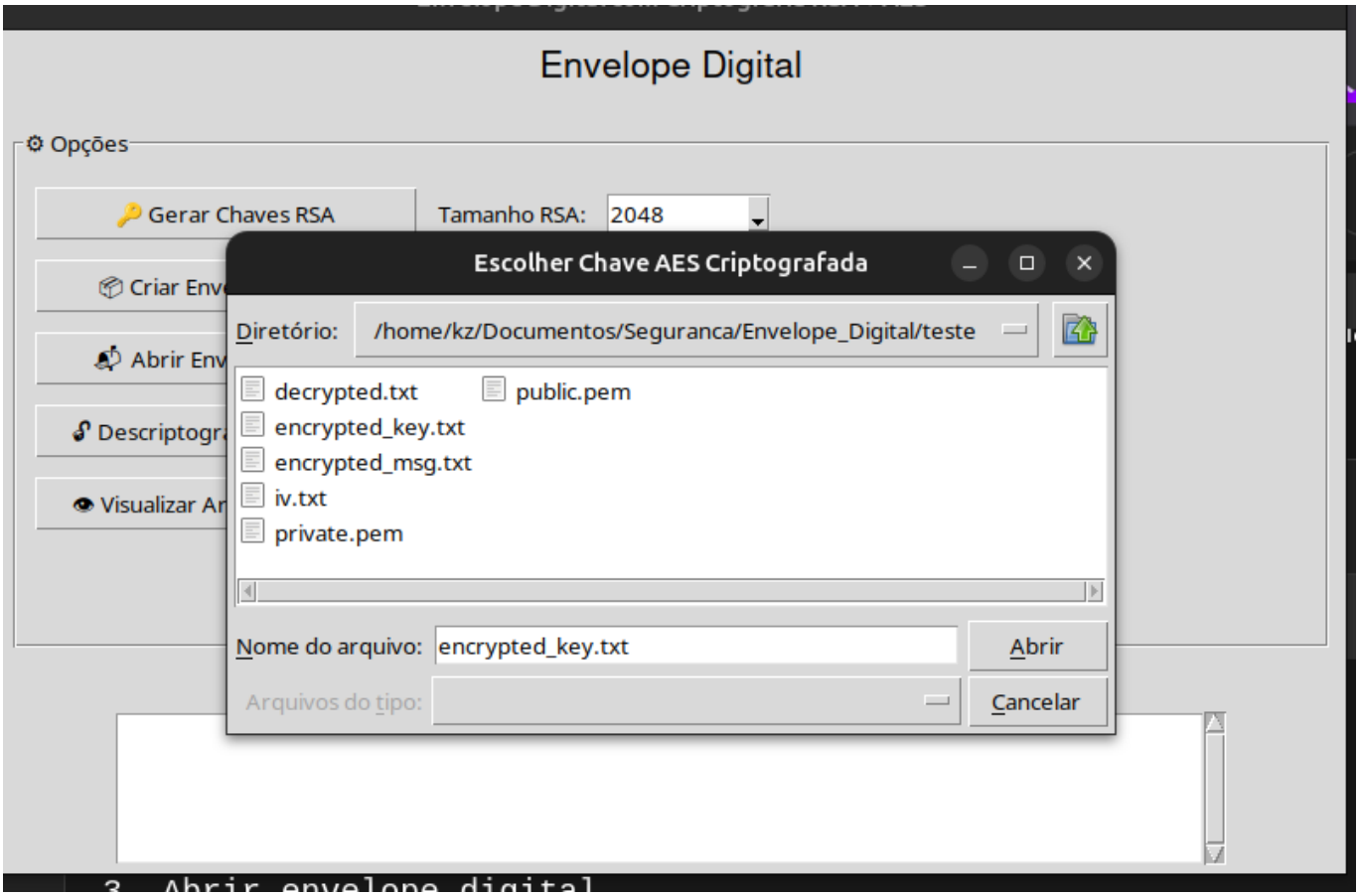

Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Escolher Chave Privada
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
private.pem
public.pem
Nome do arquivo:
private.pem
Abrir
Arquivos do tipo:
PEM files (*.pem)
Cancelar

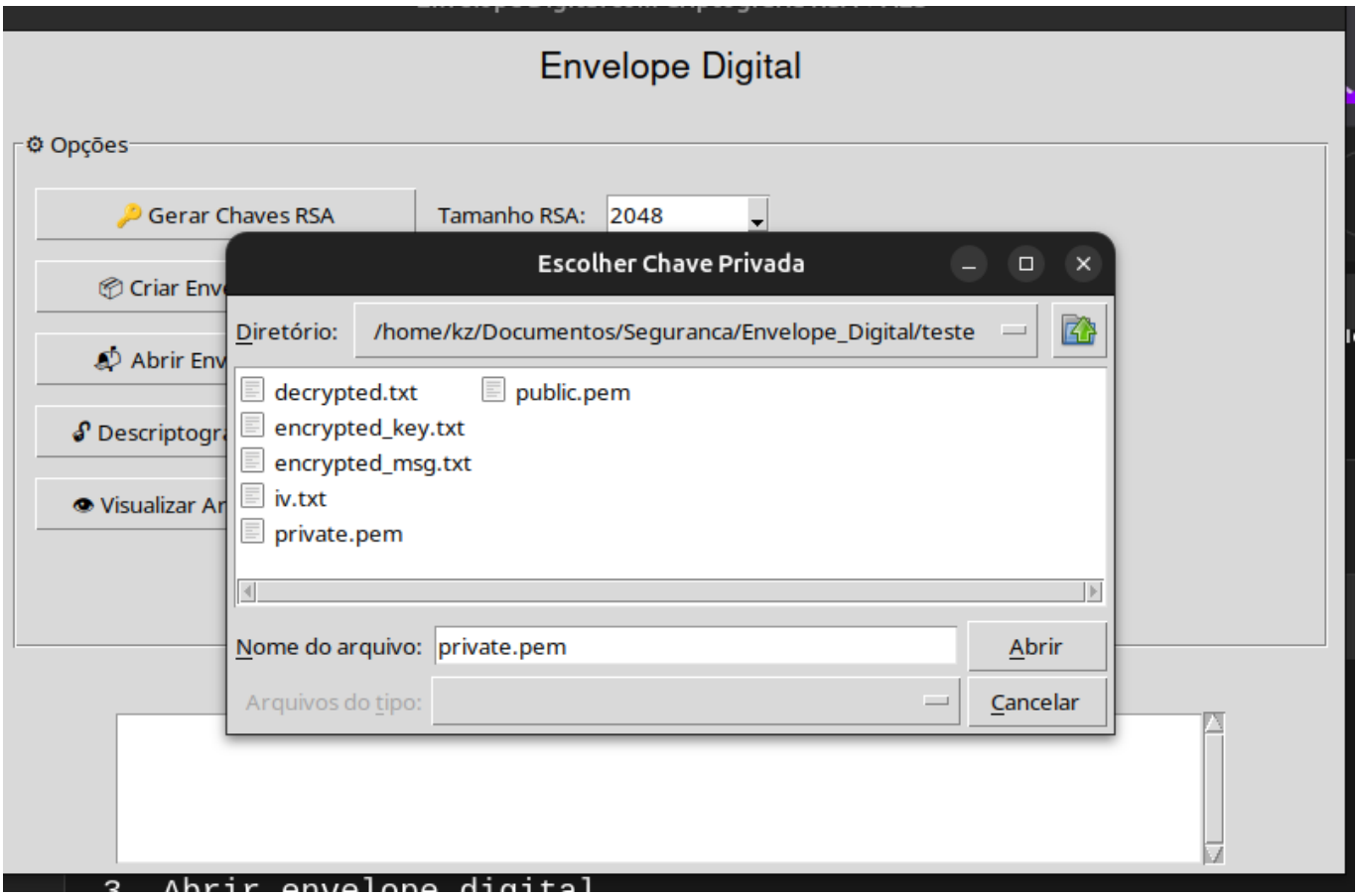

Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Escolher IV
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
encrypted_key.txt
encrypted_msg.txt
iv.txt
Nome do arquivo:
iv.txt
Abrir
Arquivos do tipo:
Text files (*.txt)
Cancelar

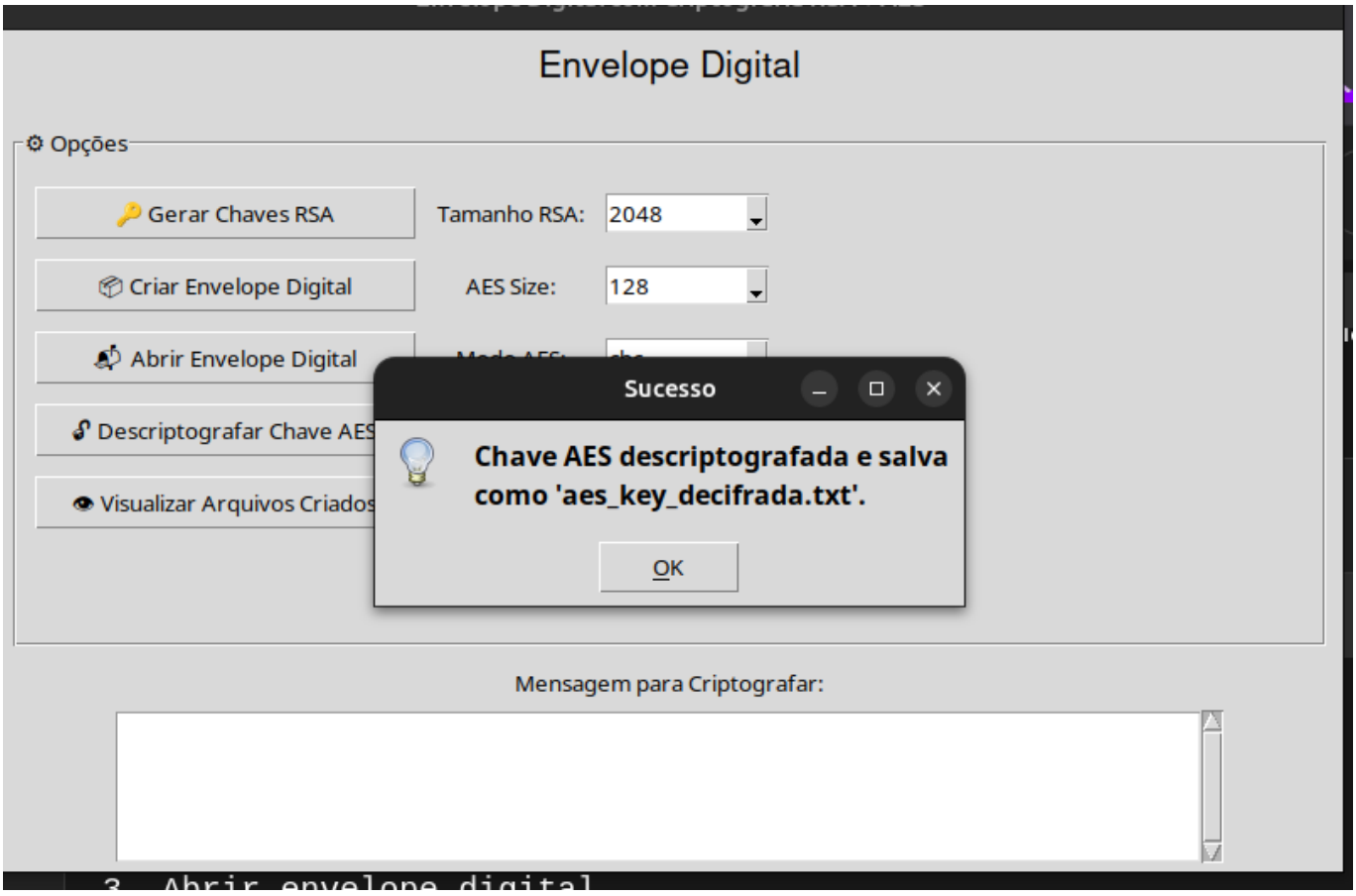




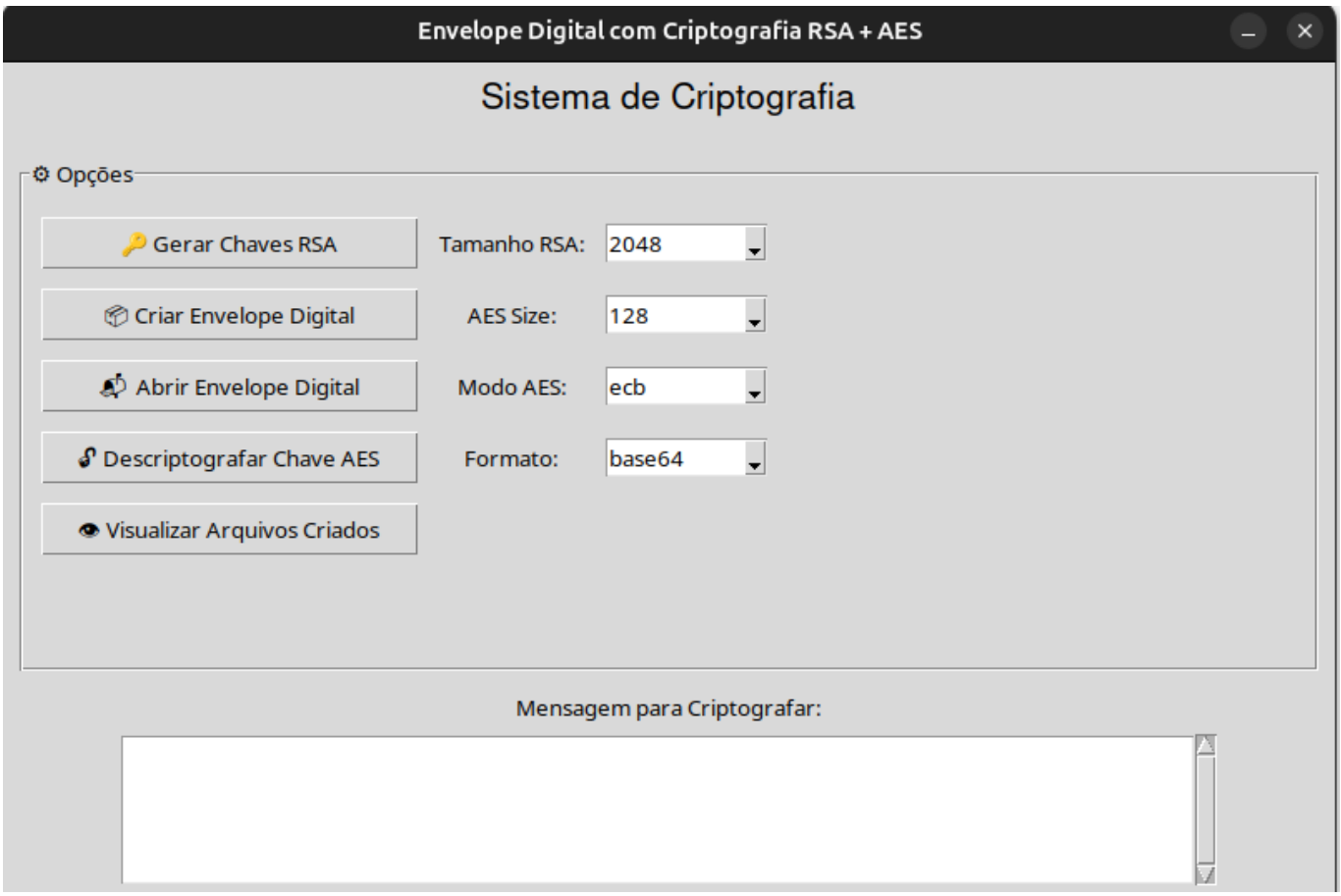
🔐 Descriptografia AES


Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Escolher Chave AES Criptografada
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
decrypted.txt
public.pem
encrypted_key.txt
encrypted_msg.txt
iv.txt
private.pem
Nome do arquivo:
encrypted_key.txt
Abrir
Arquivos do tipo:
Cancelar

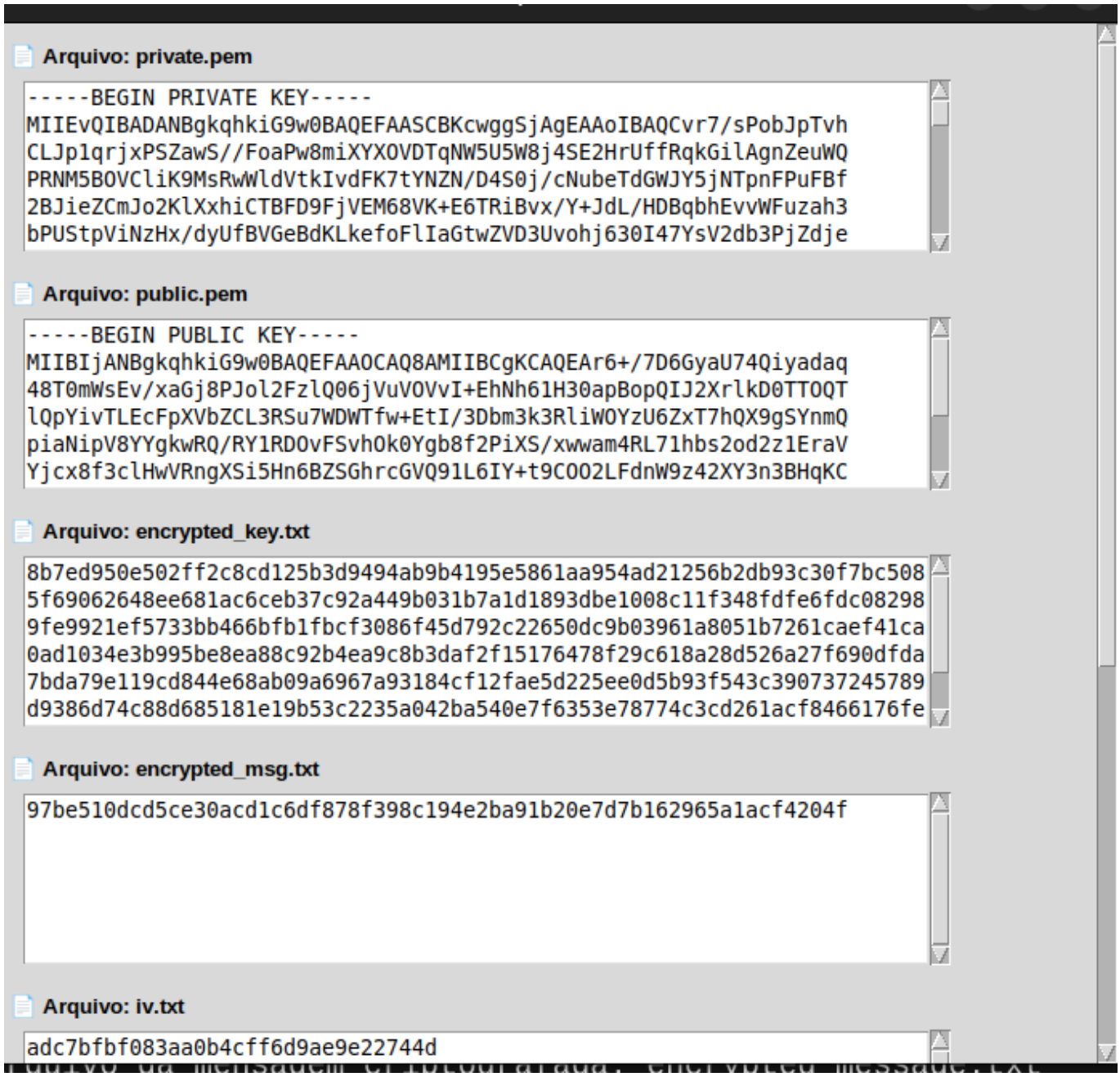

Envelope Digital
Opções
Gerar Chaves RSA
Tamanho RSA:
2048
Escolher Chave Privada
Diretório:
/home/kz/Documentos/Seguranca/Envelope_Digital/teste
decrypted.txt
public.pem
encrypted_key.txt
encrypted_msg.txt
iv.txt
private.pem
Nome do arquivo:
private.pem
Abrir
Arquivos do tipo:
Cancelar



🖥️ Interface Principal



📊 Visualização


Arquivo: private.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCvr7/sPobJpTvh
CLJp1qrjxPSZawS//FoaPw8miXYXOVDTqNW5U5W8j4SE2HrUffRqkGilAgnZeuWQ
PRNM5BOVCliK9MsRwWldVtkIvdFK7tYNZN/D4S0j/cNubeTdGWJY5jNTpnFPuFBf
2BJieZCmJo2KlXxhiCTBFD9FjVEM68VK+E6TRiBvx/Y+JdL/HDBqbhEvvWFuzah3
bPUStpViNzHx/dyUfBVGeBdKLkefoFlIaGtwZVD3Uvohj630I47YsV2db3PjZdje
Arquivo: public.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr6+/7D6GyaU74Qiyadaq
48T0mWsEv/xaGj8PJol2FzlQ06jVuVOVvI+EhNh61H30apBopQIJ2XrlkD0TTOQT
lQpYivTLEcFpXVbZCL3RSu7WDWTfw+EtI/3Dbm3k3RliWOYzU6ZxT7hQX9gSYnmQ
piaNipV8YYgkwRQ/RY1RDOvFSvhOk0Ygb8f2PiXS/xwwam4RL71hbs2od2z1EraV
Yjcx8f3clHwVRngXSi5Hn6BZSGhrcGVQ91L6IY+t9COO2LFdnW9z42XY3n3BHqKC
Arquivo: encrypted_key.txt
8b7ed950e502ff2c8cd125b3d9494ab9b4195e5861aa954ad21256b2db93c30f7bc508
5f69062648ee681ac6ceb37c92a449b031b7a1d1893dbe1008c11f348fdfe6fdc08298
9fe9921ef5733bb466bfb1fbcf3086f45d792c22650dc9b03961a8051b7261caef41ca
0ad1034e3b995be8ea88c92b4ea9c8b3daf2f15176478f29c618a28d526a27f690dfda
7bda79e119cd844e68ab09a6967a93184cf12fae5d225ee0d5b93f543c390737245789
d9386d74c88d685181e19b53c2235a042ba540e7f6353e78774c3cd261acf8466176fe
Arquivo: encrypted_msg.txt
97be510dcd5ce30acd1c6df878f398c194e2ba91b20e7d7b162965a1acf4204f
Arquivo: iv.txt
adc7bfbf083aa0b4cff6d9ae9e22744d