

# SecureFile - AES Encryptor

## Complete User Manual

---

**Version:** 1.0

**Developer:** Hamza Sami - Cybersecurity Specialist

**Contact:** [programmerhamzasami@gmail.com](mailto:programmerhamzasami@gmail.com) | Telegram: @h\_s\_y

---

### Table of Contents






1. Introduction & Overview
  2. File Encryption Guide
  3. File Decryption Guide
  4. Password Recovery Tool
  5. Technical Specifications
  6. Troubleshooting & Support
- 

## Page 1: Introduction & File Encryption

### What is SecureFile?


SecureFile is a professional-grade file encryption application that uses **AES-256 encryption** to protect your sensitive files. Whether you need to secure personal documents, business files, or confidential data, SecureFile provides military-grade encryption with an intuitive interface.

### Key Features:


-  **AES-256 Encryption** - Industry-standard security
  -  **Easy Decryption** - Simple password-based recovery
  -  **Password Recovery** - Brute-force wordlist attack capability
  -  **Universal File Support** - Encrypt any file type
  -  **Modern Interface** - Clean, professional design
- 

### File Encryption Guide


#### Step 1: Access the Encrypt Tab

- Launch SecureFile application
- Click on the " **Encrypt**" tab (highlighted in gold when selected)


## Step 2: Select Your File

1. Click the " **Browse File**" button (yellow/gold colored)
2. Navigate to and select the file you want to encrypt
3. The file path will appear in the text field above the browse button
4. **Supported Files:** All file types (documents, images, videos, archives, etc.)

## Step 3: Set Your Password

1. Click in the " **Encryption Password**" field
2. Enter a strong password (recommended: 12+ characters with mixed case, numbers, symbols)
3. **Important:** Remember this password - it cannot be recovered without the Recovery tool!

## Step 4: Encrypt & Save

1. Click " **Encrypt & Save**" button
2. Choose where to save your encrypted file
3. The file will be saved with a .enc extension
4. A success message will confirm the encryption completed


### **Security Tips:**

- Use unique, complex passwords
  - Store passwords securely (password manager recommended)
  - Keep backup copies of important encrypted files
  - The original file remains unchanged - delete it manually if needed
- 


## Page 2: File Decryption Guide

### **File Decryption Guide**


#### Step 1: Access the Decrypt Tab

- Click on the " **Decrypt**" tab in the application
- The tab will be highlighted in gold when active


## Step 2: Select Encrypted File

1. Click " **Browse Encrypted File**" button
2. Navigate to your `.enc` file (encrypted file)
3. Select the file - path will display in the text field
4. **File Filter:** The dialog will show `.enc` files by default

## Step 3: Enter Password

1. Click in the " **Decryption Password**" field
2. Enter the exact password used during encryption
3. **Case Sensitive:** Password must match exactly
4. Characters will be hidden for security (password field)

## Step 4: Decrypt & Save

1. Click " **Decrypt & Save**" button
2. Choose location to save the recovered file
3. The file will be restored with its original extension
4. Success message confirms decryption completed

### **Decryption Notes:**

- Wrong password will result in decryption failure
- Corrupted files cannot be decrypted
- Original file extension is automatically restored
- Decrypted file is identical to the original

---

## **Technical Specifications**

### **Encryption Details:**

- **Algorithm:** AES (Advanced Encryption Standard)
- **Key Size:** 256-bit
- **Mode:** CBC (Cipher Block Chaining)
- **Key Derivation:** SHA-256 hash of password
- **IV Generation:** MD5 hash of password
- **Padding:** PKCS7 padding scheme

## File Structure:

Encrypted File (.enc) = [Extension][IV][Encrypted Data]

- Extension: 8 bytes (original file extension)
- IV: 16 bytes (initialization vector)
- Encrypted Data: Variable length (padded original file)

## System Requirements:

- **OS:** Windows 7/8/10/11
  - **RAM:** 256MB minimum
  - **Storage:** 50MB free space
  - **Dependencies:** Self-contained executable
- 


## Page 3: Password Recovery & Support

### Password Recovery Tool

#### When to Use Recovery:


- Forgotten encryption password
- Suspected password with variations
- Dictionary-based password recovery

#### Step 1: Access Recovery Tab


- Click " **Recovery**" tab
- Interface shows encrypted file and wordlist selection

#### Step 2: Select Files


##### 1. Encrypted File:

- Click " **Browse Encrypted File**"
- Select your `.enc` file to crack


##### 2. Password Wordlist:

- Click " **Browse Wordlist**"
- Select a `.txt` file containing potential passwords
- Each password should be on a separate line

### Step 3: Start Recovery Process

1. Click " **Start Recovery**" button
2. Progress bar shows completion percentage
3. **Status window** displays:
  - Currently testing password
  - Progress updates
  - Error messages (if any)

### Step 4: Monitor Progress

- **Real-time Status:** Current password being tested
- **Progress Bar:** Percentage of wordlist completed
- **Stop Option:** Click " **Stop**" to halt the process
- **Success:** Found password appears in "Recovered Password" field

### Creating Wordlists:

```
password123
mypassword
123456
qwerty
admin
letmein
password1
```

### Recovery Tips:

- Use comprehensive wordlists (rockyou.txt, common passwords)
- Include password variations (numbers, capitals, symbols)
- Start with most likely passwords
- Recovery time depends on wordlist size and password position



---

## Troubleshooting & Support




### Common Issues:

#### Encryption Fails:




-  Check file permissions (read access)

-  Ensure sufficient disk space
-  Verify file is not corrupted or in use

### **Decryption Fails:**

-  Verify password is correct (case-sensitive)
-  Ensure encrypted file is not corrupted
-  Check file was encrypted with SecureFile

### **Recovery Not Working:**

-  Verify wordlist format (one password per line)
-  Check encrypted file is valid
-  Ensure wordlist contains the correct password

### **Security Best Practices:**

#### **1. Password Management:**

- Use unique passwords for each file
- Consider using a password manager
- Include special characters and numbers

#### **2. File Safety:**

- Keep backups of encrypted files
- Test decryption immediately after encryption
- Store encryption passwords securely

#### **3. Recovery Preparation:**

- Create personal wordlists with likely passwords
- Include common variations of your passwords
- Keep wordlists updated and comprehensive

---

## **Support & Contact**

**Developer:** Hamza Sami

**Specialization:** Cybersecurity

**Email:** [programmerhamzasami@gmail.com](mailto:programmerhamzasami@gmail.com)

**Telegram:** @h\_s\_y

## **Security Notice:**

SecureFile uses industry-standard AES-256 encryption. While this provides excellent security, always follow best practices for password management and file handling. The developer is not responsible for data loss due to forgotten passwords or corrupted files.

---

© 2024 SecureFile - Professional File Encryption Solution