



Secure Text & File Encryption Tool

Crypt is a lightweight, standalone Windows application built in Python (with PyQt5). It provides a secure graphical interface for encrypting and decrypting text and attachments using RSA public/private keys — optionally protected by a passphrase.

Ideal for:

- Secure personal messaging
 - Safely transmitting sensitive files
 - Practicing or testing RSA workflows
 - Lightweight encryption without needing command-line tools
-



What's Included in the ZIP Package

After extracting, you'll find:

- `crypt.exe` — Main Windows application
 - `README.txt` — This installation and usage guide
 - *(Optional)* `public_key.pem` / `private_key.pem` — Sample keys for testing
-



System Requirements

- Windows 10 or 11 (64-bit)
 - No Python installation required (Python is bundled)
 - No Internet access required
 - No installation needed — extract and run!
-

Installation Steps

1. **Extract the ZIP**
 - Right-click the .zip file → “Extract All...”
 - Choose a destination folder (e.g., C:\Users\YourName\Documents\crypt)
 2. **Bypass SmartScreen (if prompted)** Because the app is unsigned, Windows Defender may block it:
 - **Option A: Run Anyway**
 - Double-click `crypt.exe`
 - If you see “Windows protected your PC”, click:
 - **More info** → **Run anyway**
 - **Option B: Add a Defender Exception**
 - Open *Windows Security*
 - Go to *Virus & Threat Protection* → *Manage Settings*
 - Scroll to *Exclusions* → *Add or remove exclusions*
 - Click “+ Add an exclusion” → Select **File** → Choose `crypt.exe`
-

User Guide

Key Management (New!)

Click **Keys** → **Manage Keys** to:

- View all stored keypairs
- See strength (e.g., 2048 bits), and whether public/private keys exist
- **Add new keypairs** with a custom label and strength (1024/2048/4096)
- **Import** existing keys from disk
- **Export** selected keypairs
- **Delete** keys

Key files are saved under a user-defined **key storage location**:

- Set it via *Settings* → *Set Key Storage Location*
 - Public and private keys are stored in separate folders
-

Getting Started

1. **Set your key storage path** (optional)
 - Settings → *Set Key Storage Location*
 - All keys will be saved/loaded from this folder
 2. **Load Keys**
 - Choose encryption and decryption keys from dropdowns
 - Dropdowns are populated automatically from your key registry
 3. **Write or Paste a Message**
 - Type plaintext to encrypt or paste an encrypted blob for decryption
 4. **Attach a File (Optional)**
 - Click *Attach File* to include any file type (PDF, ZIP, EXE, etc.)
 - It will be encrypted along with your message
 5. **Enter a Passphrase (Optional)**
 - Adds AES-level protection in addition to RSA
 6. **Click Encrypt or Decrypt**
-

Features

File Attachments

- Any file can be securely attached and encrypted
- During decryption, you'll be prompted to save the attachment separately

Large File Handling

- When loading an encrypted file larger than 5MB:
 - You can choose to *load partially (first 5MB)* or *load fully for decryption only*
- When partial load is chosen:
 - Copy/paste is disabled to prevent app freezing
 - Decryption still functions fully

Clear Interface

- "Clear All" button resets both text fields and the passphrase

Key Management

- View and manage all keypairs from a centralized dialog
 - Visual indicators:
 - ✓ public/private present
 - Key strength in bits
 - Add, import, export, delete keys — all in one place
-

Example Workflows






Sending a Secure Message

1. Bob sets his key storage location
2. Bob loads Alice's **public key**
3. Bob types a message and optionally attaches a file
4. Bob sets a passphrase (optional)
5. Bob clicks **Encrypt**
6. Bob saves the output and sends it to Alice

Reading a Secure Message

1. Alice sets her key storage location
2. Alice loads her **private key**
3. Alice pastes the message or loads it from file
4. Alice enters the correct passphrase (if used)
5. Alice clicks **Decrypt**
6. Alice sees the decrypted message and can save the attachment

Configuration

Feature	Status
Internet needed	 No
Registry modification	 None
External communication	 None
Installation required	 No — portable
Settings saved?	 Yes (key storage path & keys)

? Troubleshooting

Problem	Solution
“Windows protected your PC”	Click <i>More info</i> → <i>Run anyway</i>
App crashes on run	Make sure all extracted files are present
Permission denied	Run <code>crypt.exe</code> as Administrator
Key not decrypting properly	Verify key matches encrypted file and passphrase is correct
Encrypted output looks cut off	Large file may be partially loaded — full decryption still works
Can't copy encrypted text	This is disabled when partial display is enabled

Support

If you encounter problems, please:

- Check if you're using the latest version
- Re-download and re-extract the app
- Ensure you've selected correct keys and passphrase

For extended help, contact the app provider directly or submit issues through the appropriate channel (e.g., GitHub or official website if available).