

Encryption Workflow



1. Key Concepts First

Term	Meaning
Public Key (.pem)	SAFE to share. Used to ENCRYPT messages.
Private Key (.pem)	SECRET. NEVER shared. Used to DECRYPT messages.
Certificate	Another word for "Public Key" file (when unsigned).

- ✓ Public Key = share freely
 - ✓ Private Key = protect completely
-

✂ 2. Setup Step — Key Generation

Both Joe and Sam must each generate their own key pair.

Who	Action
Joe	Runs Crypt → Clicks Generate Keys (choose 2048 or 4096 bits)
Sam	Runs Crypt → Clicks Generate Keys (choose 2048 or 4096 bits)

- ✓ This creates:
 - `private_key.pem` (Joe's private key)
 - `public_key.pem` (Joe's public key)
 - `private_key.pem` (Sam's private key)
 - `public_key.pem` (Sam's public key)
-



3. Sharing Public Keys

What Joe must do

Joe sends his **public_key.pem** to Sam
Joe keeps his **private_key.pem** private

What Sam must do

Sam sends his **public_key.pem** to Joe
Sam keeps his **private_key.pem** private

✓ Public keys can be sent by:

- Email attachment
- USB drive
- Cloud storage link (e.g., Dropbox, Google Drive)

✓ PRIVATE keys **must never leave their computers.**



4. Encrypting a Message

If Joe wants to send a message to Sam

1. Load Sam's **public_key.pem** (Load Public Key button)
2. Type message (optional: attach file)
3. (Optional) Add passphrase for extra protection
4. Click **Encrypt**
5. Save encrypted text to a file or copy
6. Send the encrypted text to Sam (Email, USB, cloud, etc.)

Joe's Steps

✓ Joe uses **Sam's public key** to encrypt → Only Sam can decrypt.



5. Decrypting a Message

When Sam receives the encrypted text

1. Load his own **private_key.pem**
2. Paste or load the encrypted text
3. Enter passphrase (if Joe used one)
4. Click **Decrypt**
5. See decrypted message (and optional attached file saved)

Sam's Steps

(Load Private Key button)

✅ Only Sam's **private key** can decrypt the text encrypted with his **public key**.



6. Important Rules for Joe and Sam

Rule	Why
Never share private keys	If someone gets your private key, they can impersonate you
Always verify public keys before using them	Prevent "man-in-the-middle" attacks
Always keep a backup of private key	If lost, you can no longer decrypt any messages
Always save the encrypted file if large	Do not rely on screen display for big files



7. Full Diagram View

