LC4: Simple Guide

What LC4 Does: Encrypt messages and files to send securely through any method (email, messaging, file sharing). Only someone with the right key can decrypt your content.

1. Create & Share Keys

1. Go to **Key Management** tab
2. Create a new key (RSA or ECC recommended)
3. **Export the public key** by clicking "Export Public"
4. Send this public key file (.lim) to your contacts
5. Have them import your public key in their app

2. Import Others' Keys

1. In **Key Management**, click "Import Key"
2. Select the .lim file your contact sent you
3. Now you can encrypt messages only they can read

3. Send Encrypted Messages

1. Go to **Encrypt** tab
2. Type your message or add a file
3. Select your contact's public key
4. Click "Encrypt Data"
5. Copy or download the encrypted result
6. Send through any method (email, chat, etc.)

4. Read Messages Sent To You

1. Go to **Decrypt** tab
2. Paste the encrypted message or upload the file
3. Select your private key that matches the public key they used
4. Enter your key password
5. Click "Decrypt Data"
6. View the decrypted message or download the file

Important Tips

- **Never share your private keys** - only share public keys (.lim files)
- **Always password-protect** your private keys
- The person who receives your message needs LC4 to decrypt it
- Encrypted messages can be sent through any channel - they remain secure

Common Questions

- **How do I know which key to use?** Use the key with the same name as the recipient
- **What's the difference between public and private?** Public keys encrypt, private keys decrypt
- **Can I use this for group messages?** Create separate encrypted messages for each recipient

---

Create keys, share public keys, encrypt with their key, send the message, they decrypt with their private key.