

## For Public Key Signature (PKS) page:

### 1. **Access the Page:**

- Once the program is running, click the "Basic Signatures" link in the navigation bar
- Or navigate directly to /basic-signatures in your URL

### 2. **Generate Keys:**

- Look for the "Key Generation" section
- Click the "Generate New Key Pair" button
- This will create your public and private keys
- You can copy these keys using the copy buttons provided

### 3. **Sign a Message:**

- Find the "Message Signing" section
- Enter the message you want to sign in the text input
- The message will be automatically hashed
- A digital signature will be generated using your private key
- You can copy the signature using the copy button

### 4. **Verify the Signature:**

- Look for the "Signature Verification" section
- The verification will happen automatically using your public key
- You can test tampering by clicking the "Tamper Message" button
- The verification status will show whether the signature is valid

### 5. **Learn More:**

- Scroll down to read the "Technical Explanation" section
- This explains how digital signatures work
- Includes details about the security benefits

For LSAG (Linkable Spontaneous Anonymous Group Signatures) page:

**1. Access the Page:**

- Once the program is running, navigate to /lsag in your URL
- You'll see the LSAG interface with options for group management and signing

**2. Generate Your Key Pair:**

- Click the "Generate Key Pair" button
- This will create your public and private keys
- Save these keys as you'll need them for signing

**3. Create or Select a Group:**

- To create a new group:
  - Enter a group name
  - Add group members (including their public keys)
  - Click "Create Group"
- Or select an existing group from the dropdown

**4. Sign a Message:**

- Select the group you want to sign for
- Enter your message in the text field
- Use your private key to sign
- Click "Sign Message"

**5. Verify Signatures:**

- Select a signature you want to verify
- The system will verify if it's a valid group signature
- You won't know which group member signed it

**6. Check Linkability:**

- Select two signatures to compare
- The system will tell you if they were created by the same signer
- This is done without revealing the signer's identity