User Guide for Digital Signature Website (RSA + SHA-256)

Step 1: Create a Digital Signature

1. Open the 'Generate QR' page from the dashboard.
2. Enter the message or statement to be signed.
3. Draw your signature manually on the provided canvas.
4. The system will:
   - Hash the message using SHA-256.
   - Encrypt the hash using an RSA private key.
   - Save the signature and signature image into a PDF file.
   - Generate a QR code pointing to the signed PDF file.

Step 2: Verify the Signature

1. Open the 'QR Verification' page from the dashboard.
2. Enter the Signature (Encrypted Hash), Public Key (e), and Modulus (n).
3. Click the 'Verify Signature' button.
4. The system will decrypt the signature and validate the SHA-256 hash against the message.
5. If the hash matches, the signature is considered VALID.

Additional Features:

- QR Code can be scanned to directly access the signed PDF.
- Public key and modulus can be downloaded as a .txt file.
- Timestamp is included to record the time of signing.

Technologies Used:

- RSA algorithm for asymmetric cryptography.
- SHA-256 for message hashing.
- Flask (Python) for backend server.
- FPDF for document generation.
- qrcode and PIL for QR code generation and image handling.

Limitations:

- Login or user authentication is not yet supported.

- Only supports PDF file output.
- Does not embed the signature directly into the document outside of visual and metadata form.

Usage Tips:

- Never share your public key with anyone.
- Store the PDF and public key/modulus safely.
- Always check the QR code link before sharing the document.
- Use signature verification to confirm authenticity.