PROGRAM -7

Q7) Demonstrate the usage/sending of a digitally signed document.

Step 1: Prepare the Document

- Create or open the document (e.g., PDF, Word, etc.) that you want to sign.

Step 2: Generate a Digital Certificate

- Obtain a **digital certificate** from a trusted Certificate Authority (CA) or generate one using a tool like:
    - Adobe Acrobat Sign
    - Microsoft Certificate Manager
    - OpenSSL (for self-signed certificates)

Step 3: Attach the Digital Signature

- Open the document in a signing tool (e.g., Adobe Acrobat, DocuSign, or Microsoft Word).
- Choose the **"Sign"** or **"Digital Signature"** option.
- Select your digital certificate to sign the document.
- Review the **timestamp** (if required) and ensure that the signature is properly applied.

Step 4: Verify the Signature (Optional)

- Ensure the document shows the **valid digital signature**—most software will show a signed icon and signature validity.
- Some tools may provide an option to **check for tampering** if the document was modified after signing.

Step 5: Send the Signed Document

- Send the signed document using:
    - **Email** (as an attachment)
    - **Cloud Services** (e.g., Google Drive, Dropbox, or Microsoft OneDrive)
    - **Document Workflow Platforms** (e.g., DocuSign or Adobe Acrobat Sign)

Step 6: Receiver Verification

- The recipient can open the document and verify the signature. Most PDF tools (like Adobe) or document systems will indicate if:
    - The signature is **valid**.
    - The document was **modified** after signing.

This process ensures the integrity, authenticity, and non-repudiation of the document.