

Information Security Management(ISM)

Ex.11.s DIGITAL SIGNATURE

LAB L7+L8

Name: Ankit Kumar Singh

Register No.:21BCE1247

*To understand the functioning of the Digital Signature, execute the following tasks: -*

1. Creating a digital signature for a given text file.
2. To encrypt and decrypt the text file and verify Digital Signature.

**SOFTWARE REQUIRED:** VM Virtual Box, Kali Linux OS

PROCEDURE:

# Digital Signature

A digital signature is an electronic, encrypted authentication stamp placed on digital information such as email messages, macros, or electronic documents. A signature confirms that the information originated with the signer and has not been altered.

# Executeute the commands stated below.

|  |  |  |
| --- | --- | --- |
| COMMAND | OUTPUT | DESCRIPTION |
| **openssl genrsa -des3 - out private.pem 2048** |  | Generate private key with length 2048. Now enter a passphrase, and remember that passphrase. |
| **openssl rsa -in private.pem -outform**  **PEM -pubout -out public.pem** |  | Generate public key. |

|  |  |  |
| --- | --- | --- |
| **echo**  **“lab10.pvt”>mssg.txt** |  | We will take a text file ‘mssg.txt’ which contains data ‘lab10.pvt’. |
| **openssl dgst -sha1 -sign private.pem -out sign mssg.txt** |  | Create digital signature. The below command will create a file ‘sign’ that  contains digital signature. |
| **openssl dgst -sha1 - verify public.pem - signature sign mssg.txt** |  | To verify the digital signature. |
| **openssl enc -aes-256- cbc -base64 -in mssg.txt**  **openssl enc -aes-256- cbc -base64 -in mssg.txt**  **-out out.txt** |  | Send the encrypted data to the receiver. |
| **openssl enc -aes-256- cbc -d-base64 -in out.txt**  **-out outDecrypted.txt** |  | In the receiver end, decrypt the out.txt file |
| **openssl dgst -sha1 - verify public.pem - signature sign outDecrypted.txt** |  | Verify the digital signature to check for the correctness of the file. |

RESULT

* + Learned the functioning of Digital signature.
  + successfully created the digital signature using a text file as input.
  + Then the text file and the digital signature is verified using encryption and decryption techniques.