Name : Siva Rama Krishna Nallapati
ID No : 190031154

DATABASE & SYSTEM SECURITY PRACTICAL - 5

Pre-Lab:

Q1.What is Digital Signature and what is the need of Digital Signatures?

Sol) A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature. Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents.

Q2. What are the advantages of Digital Signature?

Sol) Advantages of Digital Signatures Include :

1) Validity of Documents

2)Saves Both Cost and Time

3) Security Enhanced

4) Authenticity

5) Future Validity

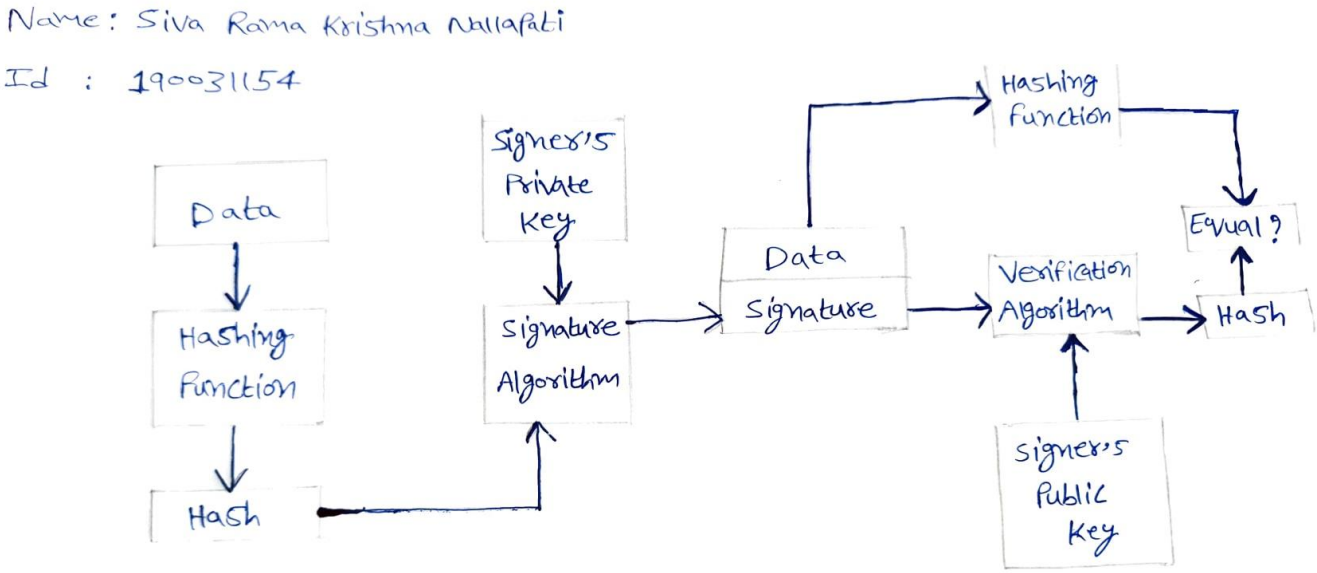
6) Customer Service Enhanced

7) Environment Friendly

Name : Siva Rama Krishna Nallapati
ID No : 190031154

Q3. Draw the model diagram for generation of Digital Signature.

Sol)



Q4.Why is the KeyPairGenerator class used in java cryptography and what are the steps to create KeyPairGenerator Class?

Sol) In java, KeyPairGenerator Class is used to generate pairs of public and private keys for the Encryption Process.

Steps to Create Key pair Generator Class :

1) Create KeyPairGenerator object using the getInstance()
2) Initialize the KeyPairGenerator object
3) Generate the KeyPairGenerator
4) Get the private key/public key

Name : Siva Rama Krishna Nallapati
ID No : 190031154

In-Lab:

Q1. Generate the Digital Signature of the file sample.txt and store the output in sample1.txt using java.

Sol)

Code / Implementation :

```
package gendigsig;
import java.io.*;
import java.security.*;
public class GenerateDigitalSignature {
	public static void main(String args[])
	{
	try
	{
	/* Generating a key pair */
	KeyPairGenerator keyGen = KeyPairGenerator.getInstance("DSA", "SUN");
	SecureRandom random = SecureRandom.getInstance("SHA1PRNG", "SUN");
	keyGen.initialize(1024, random);
	KeyPair pair = keyGen.generateKeyPair();
	PrivateKey priv = pair.getPrivate();
	PublicKey pub = pair.getPublic();
	/* Creating a Signature object and initializing it with the private key */
	Signature dsa = Signature.getInstance("SHA1withDSA", "SUN");
	dsa.initSign(priv);
	/* Updating and signing the data */
	FileInputStream fis = new FileInputStream("C:/Users/SIVA RAMA
KRISHNA/Desktop/sample.txt");
	BufferedInputStream bufin = new BufferedInputStream(fis);
	byte[] buffer = new byte[1024];
	int len;
	while (bufin.available() != 0)
	{
	len = bufin.read(buffer);
	dsa.update(buffer, 0, len);
	};
	bufin.close();

	byte[] realSig = dsa.sign();
```

Name : Siva Rama Krishna Nallapati
ID No : 190031154

```
        /* Saving the signature in a file */
        FileOutputStream sigfos = new FileOutputStream("C:/Users/SIVA RAMA
KRISHNA/Desktop/sample1.txt");
        System.out.println("Digital Signature Generated and Stored in sample1.txt");
        sigfos.write(realSig);
        sigfos.close();
        /* Saving the public key in a file */
        byte[] key = pub.getEncoded();
        FileOutputStream keyfos = new FileOutputStream("C:/Users/SIVA RAMA
KRISHNA/Desktop/publickey.txt");
        System.out.println("Public Key Generated and Stored in sample1.txt");
        keyfos.write(key);
        keyfos.close();
        }
        catch (Exception e)
        {
        System.err.println("Caught exception " + e.toString());
        }
        };
        }
```

Name : Siva Rama Krishna Nallapati
ID No : 190031154

Post-Lab:

Q1. Grant create_session_role to appsec and protect it with a password.

Sol)

```
Run SQL Command Line

SQL*Plus: Release 11.2.0.2.0 Production on Mon Mar 21 11:36:47 2022

Copyright (c) 1982, 2014, Oracle.  All rights reserved.

SQL> CONNECT System/root;
Connected.
SQL> CREATE USER appsec IDENTIFIED BY appsecpass;

User created.

SQL> GRANT create session to appsec;

Grant succeeded.

SQL>
```

Q2. Grant create procedure, create table, create view system priviliges to appsec_role.

Sol)

```
SQL> CREATE ROLE appsec_role;

Role created.

SQL> GRANT create procedure,create table, create view TO appsec_role;

Grant succeeded.

SQL>
```

Name : Siva Rama Krishna Nallapati
ID No : 190031154

Q3. Grant appsec_role to appsec

Sol)

```
SQL> GRANT appsec_role TO appsec;

Grant succeeded.

SQL>
```

Q4. To run an application, we will create an application user, appusr. numerous people will use an application, and the application will connect all of them to Oracle as our one big application user. Write a query that they do not need individual person accounts and passwords for this access

Sol)