Experiment 8

Student Name: Sahul Kumar Parida **UID: 20BCS4919**
Branch: CSE **Section/Group: WM-904/B**
Semester: 5th **Date of Performance: 08/11/2022**
Subject Name: Web and Mobile Security Lab
Subject Code: 20CSP-333

Aim:

Write a program to sign and verify a document using DSA algorithm.

Software/Hardware Requirements:

Windows 7 and above version.

Tools to be used:

1. Eclipse IDE
2. JDK (Java Development kit)
3. IntelliJ IDEA

Steps/Method/Code:

```
import java.io.*; //input the file data to be signed
import java.security.*; //provides methods for signing the data
public class GenerateDigitalSignature
{
public static void main(String args[])
{
/* Generate a DSA signature */
if (args.length != 1)
{
System.out.println("Usage: nameOfFileToSign");
}
else try
```

```
{
// the rest of the code goes here
}
catch (Exception e)
{
System.err.println("Caught exception " + e.toString());
}
}
}
```

VerifyDigitalSignature.java

```
import java.io.*;
import java.security.*;
import java.security.spec.*;
public class VerifyDigitalSignature
{
public static void main(String args[])
{
/* Verify a DSA signature */
if (args.length != 3) {
System.out.println("Usage: VerifyDigitalSignature " +"publickeyfile signaturefile " + "datafile"
);
}
else try
{
// the rest of the code goes here
}
catch (Exception e)
{
System.err.println("Caught exception " + e.toString());
}
}
}
```

Output:

Output

```
java -cp /tmp/Fuqck5lzHO GenerateDigitalSignature
Usage: nameOfFileToSign
```

Output

```
java -cp /tmp/Fuqck5lzHO VerifyDigitalSignature
Usage: VerifyDigitalSignature publickeyfile signaturefile datafile
```

Learning Outcomes:

With this, you have understood the importance of asymmetric cryptography, the working of digital signatures, the functionality of DSA, the steps involved in the signature verification, and its advantages over similar counterparts.