Experiment 3.1

Student Name: Lipakshi
Branch: CSE
Semester: 5
Subject Name: Web & Mobile Security Lab

UID: 20BCS5082
Section/Group: 20BCS-WMS-607 B
Date of Performance: 10 October 2022
Subject Code: 20CSP - 338

Aim:

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

Objective:

To generate the concept of digital signature

Hardware Requirements:

1. Computer System/Laptop having Windows 7 or above Operating Software

Software Requirements:

1. Java Development Kit (JDK)
2. IntelliJ IDEA

Introduction

What is a Digital Signature?

The **digital signature** is a mechanism that verifies the authority of digital messages as well as documents. It is very popular because it provides more security than other signatures. In Java, **JDK Security API** is used to create and implement digital signatures. In this section, we will discuss the **digital signature** mechanism and also implement the **digital signature mechanism in a Java program.**

The digital signature is an electronic signature to sign a document, mail, message, etc. It validates the authenticity, and integrity of a message or document. It is the same as a handwritten signature, seal, or stamp. It is widely used to verify digital messages, financial documents, identity cards, etc.

Advantages of Digital Signature

- Added Security
- Independent Verification
- Provides a High Standard
- Legal Compliance
- Global Acceptance
- Time Saving
- Cost Saving
- Traceability

Uses of Digital Signature

Digital signatures are used in the following areas:

- Government Sectors
- Manufacturing
- Healthcare
- Financial Services
- Crypto Currencies

Code

```
package experiments;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.Signature; import
java.util.Scanner;
public class DigitalSignature
{
public static void main(String args[]) throws Exception
{
// Taking a user input for text message signature signing
Scanner scan = new Scanner(System.in);
System.out.print("Enter your message: ");
String msg = scan.nextLine();
// Creating KeyPair generator object
KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");
// Initializing the key pair generator
keyPairGen.initialize(2048);
// Generating the pair of keys
KeyPair pair = keyPairGen.generateKeyPair();
// Getting the private key from the key pair
PrivateKey privKey = pair.getPrivate();
// Creating a Signature object
Signature sign = Signature.getInstance("SHA256withDSA");
// Initialize the digital signature
sign.initSign(privKey);
byte[] bytes = "msg".getBytes();
// Integrating data to the signature
sign.update(bytes);
// Calculating the signature
byte[] signature = sign.sign();
// Displaying the signature
System.out.print("Digital Signature: "+ new String(signature, "UTF8"));
}
```

Code Output

```
Problems  Javadoc  Declaration  Console ×
<terminated> DigitalSignature [Java Application] C:\Program Files\Java\jdk-18.0.2.1\bin\javaw.exe  (06-Nov-2022,
Enter your message: Thing of beauty is a joy forever.
Digital Signature: 0<□,?]Cq□X ?>SX?□H?C??□□~|ItC□&?+□???dRS??   ?ovgF?R_:??V?□?
```

Learning Outcomes

1. Learnt about Digital Signature Algorithms
2. Learnt about SHA256 Encryption Technique
3. Learnt about Public and Private Key Generation

Evaluation Grid:

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.			
2.			
3.			
4.			