

**UNIVERSITY INSTITUTE OFENGINEERING**

**Department of Computer Science & Engineering**

**Subject Name:** Web and Mobile Security Lab

**Subject Code:** 20CSP-338

**Submitted to: Submitted by:**

Er. Himanshi Name: Sahil Kaundal

UID: 21BCS8197

Section: 616

Group: A

**INDEX**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ex. No** | **List of Experiments** | **Conduct (MM: 12)** | **Viva**  **(MM: 10)** | **Record (MM: 8)** | **Total**  **(MM: 30)** | **Remarks/Signature** |
| 1.1 | Open any website on computer system and identify http packet on monitoring tool like Wireshark. |  |  |  |  |  |
| 1.2 | Design a method to simulate the html injection and cross site scripting to exploit the attackers. |  |  |  |  |  |
| 1.3 | Implementation of Cross site request forgery (XSRF) attack. |  |  |  |  |  |
| 2.1 | Implementation of Design methods to break authentication schemes (SQL Injection attack). |  |  |  |  |  |
| 2.2 | Program to generate message digest for the given message using the SHA/MD5 algorithm and verify the integrity of message. |  |  |  |  |  |
| 2.3 | Perform Penetration testing on a web application to gather information about the system (Foot Printing) |  |  |  |  |  |
| 2.4 | Implementation of Session hijacking attack on http-enabled website. |  |  |  |  |  |
| 3.1 | Write a program to sign and verify a document using DSA algorithm. |  |  |  |  |  |

**Experiment 8**

**Student Name:** Sahil Kaundal **UID:** 21BCS8197

**Branch:** BE CSE (Lateral Entry) **Section/Group:** 616/A

**Semester:** 5th **Date of Performance:** 12/11/2022

**Subject Name:** WMS Lab **Subject Code:** 20CSP-338

1. **Aim/Overview of the practical:**

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

1. **Task to be done/ Which logistics used:**

To generate the concept of digital signature

**3. Apparatus / Simulator Used:**

* Windows 7 & above version.
* Google Chrome C/C++
* Java
* Python platform

**Discussion:**

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, messages, etc. It

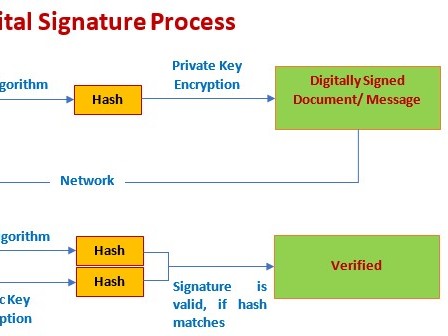
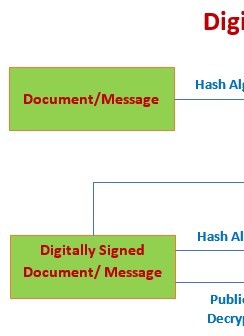
validates the authenticity, and integrity of a message or document. It is the same as a handwritten signature, seal, or stamp. It is widely used to verify a digital message, financial documents, identity cards, etc.

In short, we can say that it en ures the following:

o Integrity: It ensures the message or a document cannot be altered while transmitting.

o Authenticity: The author of the message is really who they claim to be.

o Non-repudiation: The author of the message can't later deny source.



**4. Program/ Steps/ Method:**

1. **import** java.io.\*; //input the file data to be signed
2. **import** java.security.\*; //provides methods for signing the data
3. **public class** GenerateDigitalSignature 4. {

5. **public static void** main(String args[]) 6. {

1. /\* Generate a DSA signature \*/
2. **if** (args.length != 1) 9. {

10. System.out.println("Usage: nameOfFileToSign");

11. }

12. **else try**

13. {

14. // the rest of the code goes here

15. }

16. **catch** (Exception e)

17. {

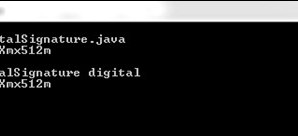
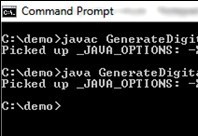
18. System.err.println("Caught exception " + e.toString());

19. }

20. }

21. }

**5. DBMS Script/Result/Output/Writing Summary:**



**VerifyDigitalSignature.java**

1. **import** java.io.\*;
2. **import** java.security.\*;
3. **import** java.security.spec.\*;
4. **public class** VerifyDigitalSignature 5. {

6. **public static void** main(String args[]) 7. {

1. /\* Verify a DSA signature \*/
2. **if** (args.length != 3) {
3. System.out.println("Usage: VerifyDigitalSignature " +"publickeyfile signaturefile " + "datafil e");

11. }

12. **else try**

13. {

14. // the rest of the code goes here

15. }

16. **catch** (Exception e)

17. {

18. System.err.println("Caught exception " + e.toString());

19. }

20. }

21. }

**Learning outcomes (What I have learnt):**

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.

**Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):**

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Parameters | Marks Obtained | Maximum Marks |
| 1. |  |  |  |
| 2. |  |  |  |