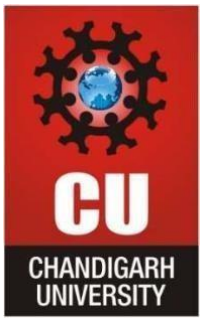
DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.



UNIVERSITY INSTITUTE OF ENGINEERING

Department of Computer Science & Engineering

Subject Name: Web And Mobile Security Lab

Subject Code: 20CSP-338

Submitted to: Renuka Ratten

Faculty name: Renuka Ratten

Submitted by: Pranjal Kumar

Name: Pranjal Kumar

UID: 20BCS3504

Section: 607

Group: B

Ex. No	List of Experiments	Conduct (MM: 12)	Viva (MM: 10)	Record (MM: 8)	Total (MM: 30)	Date	Remarks/Signature
1.1	Open any website on computer system and identify http packet on monitoring tool like Wireshark.					19/08/22	
1.2	Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.					28/08/22	
1.3	Implementation of Cross site request forgery (XSRF) attack.					16/09/22	
1.4	Implementation of Design methods to break authentication schemes (SQL Injection attack).					04/10/22	
2.1	Write a program to generate message digest for the given message using the SHA/MD5 algorithm and verify the integrity of message.					19/10/22	
2.2	Perform Penetration testing on a web application to gather information about the system (Foot Printing).					03/11/22	
2.3	Implementation of Session hijacking attack on http-enabled website and to Identify vulnerable session cookies.					04/11/22	
3.1	write a program to sign and verify a document using DSA algorithm.					05/11/22	

Experiment 3.1

Student Name: Pranjal Kumar **UID: 20BS3504**

Branch: CSE **Section/Group: 607-B**

Semester: 5th **Date of Performance: 20/10/22**

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

Aim:

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

Objective:

To generate the concept of digital signature Software/Hardware Requirements: 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.

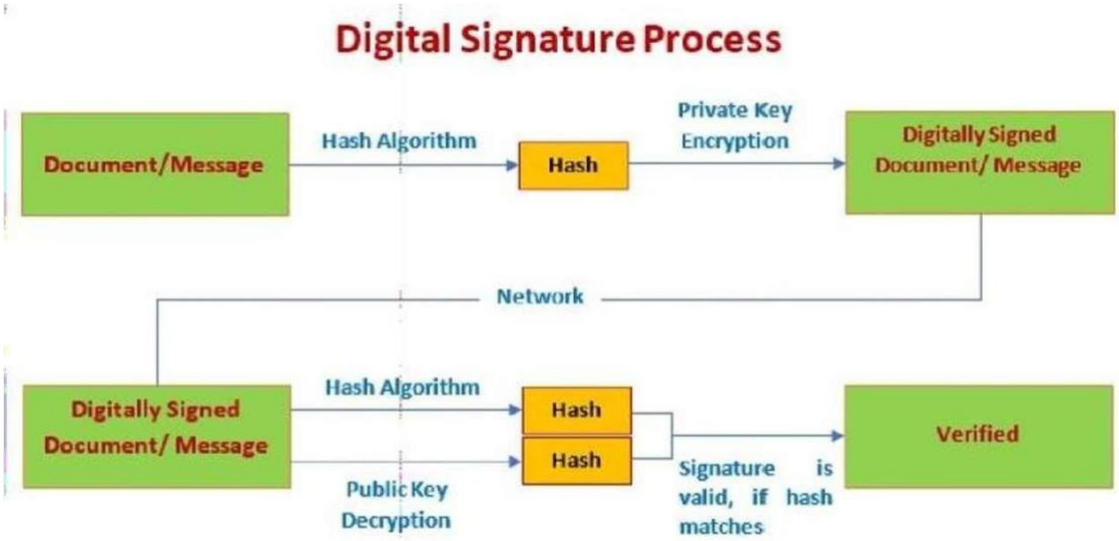
In Java, JDK Security API is used to create and implement digital signatures. In this section, we will discuss the digital signature mechanism and also implement the digital signature mechanism in a Java program.

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 ensures the following:

- **Integrity:** It ensures the message or a document cannot be altered while transmitting.
- **Authenticity:** The author of the message is really who they claim to be.

- **Non-repudiation:** The author of the message can't later deny that they were the source.



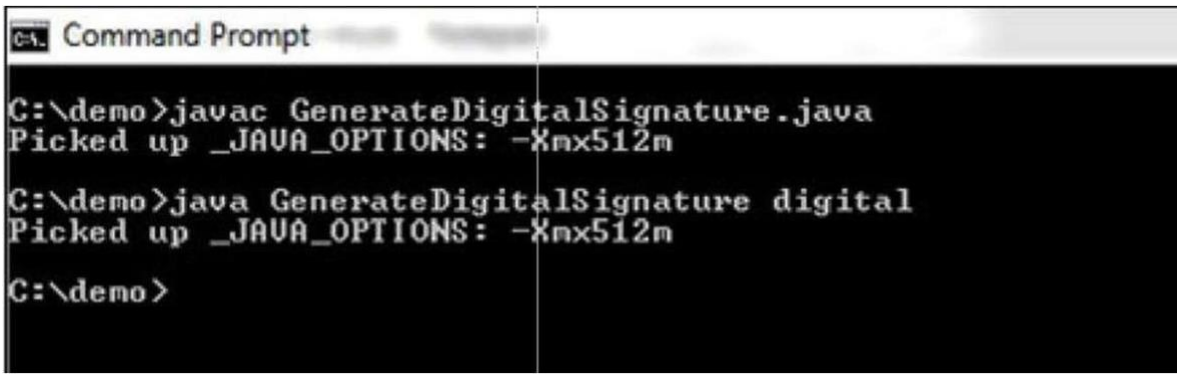
Examples:

Steps/Method/Code:

```
import java.io.*;  import java.security.*;
public class GenerateDigitalSignature { public static void
main(String args[]) { 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());
}
```

```
}
}
```

Output Screenshot:



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 " + "datafil e");
}
else try{
// the rest of the code goes here
}
catch (Exception e){
```

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

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.

Evaluation Grid :

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30