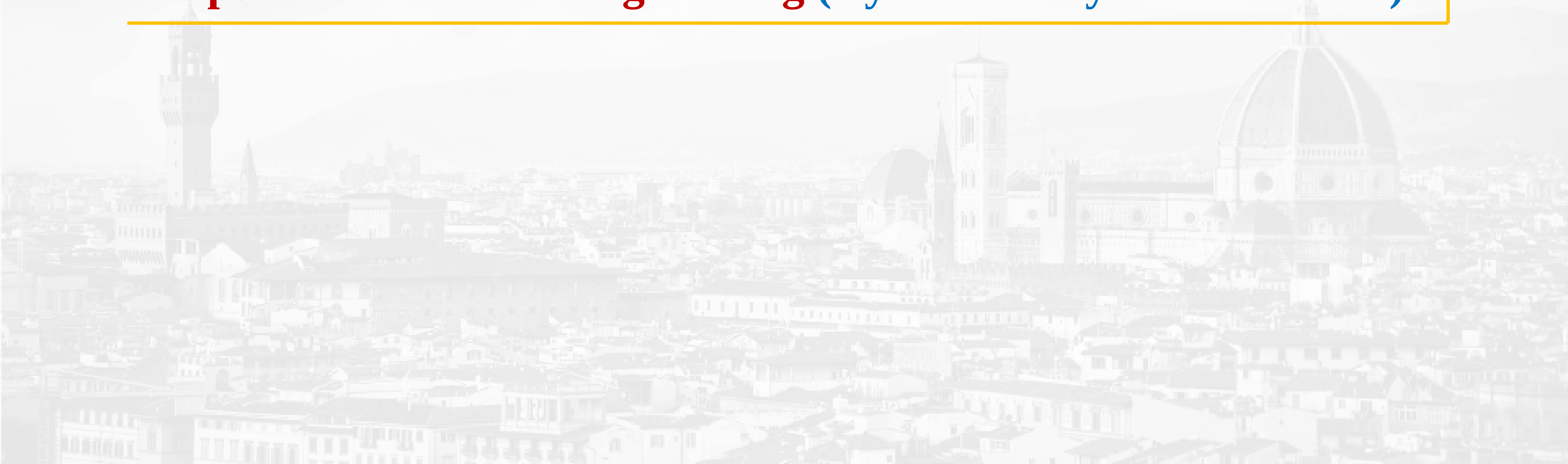
MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

SY B.Tech Semester-IV (AY 2022-23)

Computer Science and Engineering (Cybersecurity and Forensics)



Assign No.	List of Assignments
1.	Write a program using JAVA or Python or C++ to implement any classical cryptographic technique.
2.	Write a program using JAVA or Python or C++ to implement Feistal Cipher structure
3.	Write a program using JAVA or Python or C++ to implement S-AES symmetric key algorithm.
4.	Write a program using JAVA or Python or C++ to implement RSA asymmetric key algorithm.
5.	Write a program using JAVA or Python or C++ to implement integrity of message using MD5 or SHA
6.	Write a program using JAVA or Python or C++ to implement Diffie Hellman Key Exchange Algorithm
7.	Write a program using JAVA or Python or C++ to implement Digital signature using DSA.
8.	Demonstrate Email Security using - PGP or S/MIME for Confidentiality, Authenticity and Integrity.
9.	Demonstration of secured web applications system using SSL certificates and its deployment in Apache tomcat server
10.	Configuration and demonstration of Intrusion Detection System using Snort.
11.	Configuration and demonstration of NESSUS tool for vulnerability assessment.

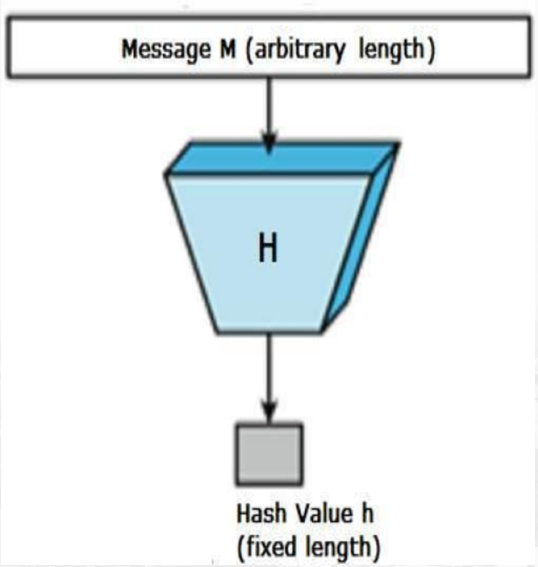
Write a program using JAVA or Python or C++ to implement integrity of message using MD5 or SHA

Objectives:

- ❖ To check the data integrity

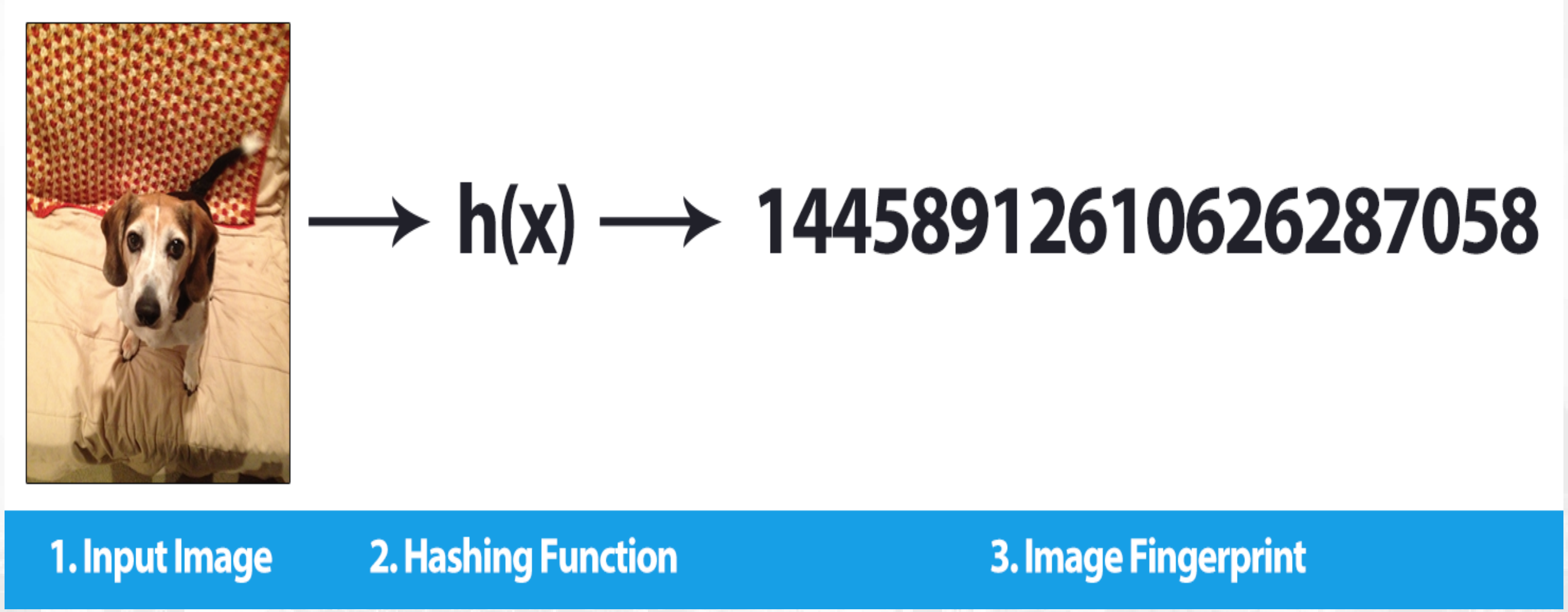
Algorithm

- The digest is sometimes called the "hash" or "fingerprint" of the input.
- Hash value is used to check the integrity of the message



Algorithm:

- Step -1: Padding
- Step - 2: Append length
- Step - 3: Divide the input into 512-bit blocks.
- Step - 4: Initialize chaining variables (4 variables: MD-5/ 5 variables: SHA-1)
- Step - 5: Process blocks



→ h(x) → 14458912610626287058

1. Input Image 2. Hashing Function 3. Image Fingerprint

INPUT/OUTPUT

Enter the original image/text/audio/video:

Calculate hash value :x

Enter the new image/text/audio/video you want to check for tampering:

Calculate hash value :y

Check image tampering : x == y

Original hash: bfb31b6eecc0c00229dd49ae71862133

New hash: bfb31b6eecc0c00229dd49ae71862133

Image not tampered

Rotate the image

Original hash: bfb31b6eecc0c00229dd49ae71862133

New hash: 1442ef1e1ff27e5319e396377625ff20

!!!!!!!!Image tampered!!!!!!!