

Practical Homework On Digital Signatures & Authentication

Objective

In this practical, students will use two virtual machines (VMs) to:

- ◆ Generate and use digital signatures.
- ◆ Verify message integrity and authentication.
- ◆ Understand how cryptographic tools work in real systems.

Deadline

- ◆ April 12

Required Setup

Each student will need:

- ◆ A VM running Linux.
- ◆ **GnuPG (GPG)** installed for encryption and signing:
 - ◆ `sudo apt install gnupg`
- ◆ A second VM to exchange signed messages.



Task 1: Generate and Share a GPG Key Pair

Deliverables:

- ◆ Screenshot of key generation.
- ◆ Screenshot of importing a partner's key.



Task 2: Sign a Message and Verify the Signature in the Second Machine

Deliverables:

- ◆ Screenshot of signing a message.
- ◆ Screenshot of verifying the received signature.
- ◆ Short discussion response.



Task 3: Encrypt and Decrypt a Message

Deliverables:

- ◆ Screenshot of encrypting a message.
- ◆ Screenshot of decrypting the received message.
- ◆ Confirmation message from the partner.



Task 4: Secure a File Transfer with Encryption & Integrity Check

Deliverables:

- ◆ Screenshot of encrypting and signing the file.
- ◆ Screenshot of decrypting and verifying it.
- ◆ Short discussion response.



Task 5: Final Analysis

Instructions:

Write a short report (1-2 pages) answering the following questions:

1. Message Integrity & Authentication:

- ◆ How does signing a message ensure authenticity?
- ◆ What happens when a message is modified after signing?

2. Encryption & Confidentiality:

- ◆ Why is encrypting messages important?
- ◆ How does encryption differ from digital signatures?

3. Real-World Applications of Digital Signatures:

- ◆ Where are digital signatures used in real life?
- ◆ Find one case where a lack of digital signatures led to fraud.



Submission Requirements

Each student must submit:


- ◆ Screenshots for all tasks.
- ◆ Short responses for each section of Task 5.



Rubric

Task 1: Generate and Share a GPG Key Pair – 10%

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
Key Generation	Screenshot clearly demonstrates successful key generation with all necessary details shown.	Screenshot shows key generation but lacks some detail or clarity.	Screenshot of key generation is unclear or missing some information.	No screenshot or incorrect key generation process shown.
Importing a Partner's Key	Screenshot clearly shows the partner's key being imported, with all necessary steps followed.	Screenshot shows key import but lacks some clarity or detail.	Screenshot is unclear, or some important steps are missing in the process.	No screenshot or key import process is not shown.





Task 2: Sign a Message and Verify the Signature in the Second Machine – 20%

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
Signing the Message	Screenshot clearly demonstrates the message signing process with proper context and settings.	Screenshot of signing is provided but with minor issues or unclear steps.	Screenshot is unclear or lacks essential information about signing.	No screenshot or signing process is incorrect or incomplete.
Verifying the Signature	Screenshot clearly demonstrates verification of the signature, with all necessary steps.	Verification is shown but lacks clarity or some minor details.	Verification process is unclear, missing key details or steps.	No verification process provided, or incorrect steps shown.
Discussion Response	Provides a clear and thoughtful explanation, detailing the signing and verification process with insights.	Provides a reasonable explanation but lacks depth or full clarity.	Discussion is vague, minimal, or lacks depth in explaining the process.	No or unclear discussion provided.



Task 3: Encrypt and Decrypt a Message – 20%

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
Message Encryption	Screenshot clearly shows the encryption process with all	Screenshot of encryption is provided but	Screenshot of encryption lacks clarity, or some	No screenshot, or encryption is performed incorrectly.

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
	necessary details.	with minor clarity issues.	key steps are missing.	
Message Decryption	Screenshot clearly demonstrates successful decryption, showing all correct steps.	Decryption is shown but lacks full clarity or minor steps are unclear.	Screenshot is unclear, or steps of decryption are missing or incorrect.	No decryption screenshot or incorrect decryption process.
Partner Confirmation	Confirmation message from partner is clear and shows the received, decrypted message.	Confirmation message is provided, but lacks clarity or full context.	Confirmation is vague or incomplete, lacking sufficient context.	No confirmation provided from the partner.



Task 4: Secure a File Transfer with Encryption & Integrity Check – 20%

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
File Encryption and Signing	Screenshot clearly demonstrates file encryption and signing with correct steps.	Screenshot provided but may lack some details or clarity in the process.	Screenshot is unclear, missing key steps, or incorrect.	No screenshot or incorrect process for file encryption/signing.
Decryption and Verification	Screenshot clearly shows file decryption and verification with correct steps.	Decryption and verification are shown but with some unclear or	Process is unclear, missing key steps or incorrectly demonstrated.	No screenshot or incorrect decryption/verification process shown.

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
		missing details.		
Discussion Response	Provides a well-thought-out, detailed response with clear insights into the encryption and verification process.	Provides a clear but less detailed discussion with minor issues.	Response is unclear, missing details, or lacks depth.	No discussion or poorly explained.



Task 5: Final Analysis – 30%

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
Message Integrity & Authentication	Comprehensive, insightful answers that clearly explain the role of digital signatures in ensuring authenticity and integrity.	Answers are clear and address the main points, but lack full detail or depth.	Answers are vague or partially incorrect.	Answers are incomplete, unclear, or incorrect.
Encryption & Confidentiality	In-depth, well-explained answers, demonstrating a clear understanding of encryption vs. digital signatures.	Answers are clear but lack full details or key comparisons between encryption and digital signatures.	Answers are minimal, vague, or incomplete.	Answers are incomplete, irrelevant, or incorrect.
Real-World Applications	Thorough, well-researched real-	Provides clear	Examples are vague or lack	Examples are missing or

Criteria	Excellent (90-100%)	Good (70-89%)	Needs Improvement (50-69%)	Unsatisfactory (0-49%)
	world examples of where digital signatures are used, and clear case analysis of fraud.	examples, but lacks depth or detailed analysis of a fraud case.	sufficient explanation.	incorrect.



Contact

For any questions or technical assistance, please reach out via **Teams** or email:

OSAMA RAFAT ALKARNAWI (s202183150@kfupm.edu.sa )

Documentation

For further details, refer to the [GnuPG Documentation](#) .

