Ain Shams University
Faculty of Engineering
Computer and Systems Eng. Dept.
CHEP- Fall 2024

CSE451: Computer and Network Security
Project Specifications

Secure Communication Suite: A Cryptography Application in Python

1. **This is a group (3-4 students) project,**
2. **Only one member of the group is required to submit.**

Title: Secure Communication Suite: A Cryptography Application in Python

Project Description: This project aims to develop a **Secure Communication Suite** in Python, a comprehensive application that integrates various cryptographic techniques and security protocols. The suite will feature **block ciphers** for symmetric encryption, **public key cryptosystems** for asymmetric encryption, and **hashing functions** for data integrity. It will also incorporate **key management** solutions for secure key distribution and storage, and **authentication** mechanisms to verify user identities. The application will be designed to secure **internet services**, protecting data in transit and at rest.

Features and Specifications:

- **Block Cipher Module:** Implement AES or DES for symmetric encryption.
- **Public Key Cryptosystem Module:** Implement RSA or ECC for asymmetric encryption.
- **Hashing Module:** Implement SHA-256 or MD5 for data integrity checks.
- **Key Management Module:** Develop secure methods for key generation, distribution, and storage.
- **Authentication Module:** Implement password-based or certificate-based authentication mechanisms.
- **Internet Services Security Module:** Apply the cryptographic modules to secure data for internet services.

User Stories:

- As a user, I want to encrypt my messages using a block cipher so that they can be securely transmitted.
- As a user, I want to use public key cryptosystems to securely share keys with my communication partner.
- As a user, I want to verify the integrity of my received messages using hashing functions.
- As a user, I want to manage my cryptographic keys securely.
- As a user, I want to authenticate myself to the system to ensure secure access.
- As a user, I want to secure my internet services using the provided cryptographic modules.

Skeleton Python Code

```
import threading
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes

class EncryptionWorker(threading.Thread):
    def __init__(self, plaintext_queue, ciphertext_queue):
        threading.Thread.__init__(self)
        self.plaintext_queue = plaintext_queue
        self.ciphertext_queue = ciphertext_queue
        self.key = get_random_bytes(16)  # AES key must be either 16, 24, or 32 bytes long
        self.cipher = AES.new(self.key, AES.MODE_EAX)

    def run(self):
        while True:
            plaintext = self.plaintext_queue.get()
            if plaintext is None:
                break
            ciphertext, tag = self.cipher.encrypt_and_digest(plaintext)
            self.ciphertext_queue.put((ciphertext, tag))

# Usage:
# plaintext_queue = queue.Queue()
# ciphertext_queue = queue.Queue()
# worker = EncryptionWorker(plaintext_queue, ciphertext_queue)
# worker.start()
# ...
# worker.join()
```

This code defines a worker thread that encrypts plaintext messages using AES. The plaintext messages are retrieved from a queue, and the resulting ciphertext is put into another queue. This allows for easy integration with other parts of your project, as you can simply add plaintext messages to the queue and retrieve the encrypted messages from the other queue.

Project Phases

Phase 1: Design and Planning

- Deliverables: Project plan, software requirements specification, and design documents.
- Questions to be answered by the end of this phase:
    1. What are the key components of the Secure Communication Suite?
    2. What cryptographic techniques will be used in the project?
    3. What are the main functions of each module in the suite?

Phase 2: Development of Cryptographic Modules

- Deliverables: Working code for block cipher, public key cryptosystem, and hashing modules.
- Questions to be answered by the end of this phase:
    1. How does the block cipher module work?
    2. What is the role of the public key cryptosystem module?
    3. How does the hashing module ensure data integrity?

Phase 3: Development of Key Management and Authentication Modules

- Deliverables: Working code for key management and authentication modules.
- Questions to be answered by the end of this phase:
    1. How does the key management module secure key distribution and storage?
    2. What authentication mechanisms are implemented in the authentication module?
    3. How does the authentication module verify user identities?

Phase 4: Integration and Testing

- Deliverables: Fully integrated Secure Communication Suite, test cases, and test results.
- Questions to be answered by the end of this phase:
    1. How are the different modules integrated into the Secure Communication Suite?
    2. What types of tests were conducted on the suite?
    3. How does the suite secure internet services?

Remember, each phase should follow proper software engineering practices, including version control, code reviews, and regular team meetings. Also, each phase should end with a presentation and demonstration of the deliverables to ensure understanding and to get feedback. Good luck with your project!

Submission Guidelines:

- **Due Date:** Saturday, December 21, 2024
- **Format:** Submit the final report as a Word and PDF + project code as zip file
- **Assessment Criteria:** The project will be assessed based on completeness, adherence to the problem statement, research methodology, inclusive of information, creativity, and quality of documentation.

PPT marking criteria

Course Code:	.....	**Course Name:**	.....	**Assignment No.**	.....	**Date:**	.....
Student Name:	.....			Student ID:	.....		

	A (89-100)				B (76-88)				C (67-75)				D (60-66)				F (0-59)			
	100	96	92	89	88	84	80	76	75	72	69	67	66	64	62	60	59	49	20	0
Relevance & Organization of Ideas (50%)	• Materials cover the topic widely & deeply. • All main points fully developed. No repetition				• Materials cover the topic widely & deeply. • Clearly structured. All main points valid but not always fully developed. Minor repetition or deviation.				• Most of the materials cover the topic reasonably. • Some structure. Most but not all main points valid & developed. Some repetition.				• Some of the materials are relevant and slightly cover the topic. • Structure not clear. Few valid main points. Repetition or deviation.				• Materials do not cover the topic. • Unstructured. Few, if any, valid main points. Material mostly deviated from the task. Inaccurate or absent.			
Answering Questions (30%)	• Answers are correct and to the point.				• Most answers are correct.				• Some answers are correct.				• Few answers are correct.				• Most answers are incorrect.			
Presentation Language (20%)	• Excellent ability to express ideas with proper language and technical vocabulary.				• Good ability to express ideas with proper language and technical vocabulary.				• Normal ability to express ideas with proper language and technical vocabulary.				• Low ability to express ideas with proper language and technical vocabulary.				• Difficult to express ideas with proper language and technical vocabulary.			

Ain Shams University
Faculty of Engineering
Computer and Systems Eng. Dept.
CHEP- Fall 2024

Report marking criteria

Course Code:	.....	**Course Name:**	.....	**Assignment No.**	.....	**Date:**	.....
Student Name:	.....			Student ID:	.....		

	A (89-100)				B (76-88)				C (67-75)				D (60-66)				F (0-59)			
	100	96	92	89	88	84	80	76	75	72	69	67	66	64	62	60	59	40	20	0
Literature survey (25%)	• Critical evaluation and synthesis of relevant issues and materials				• Critical evaluation of relevant issues and materials				• Accurate description of main relevant issues				• Limited evaluation and description of main issues				• Insufficient and largely irrelevant material			
Research Objectives (25%)	• Clearly defined research problem with well-structured research objectives				• Complete set of research objectives				• Limited research objectives				• Poorly defined objectives				• Research problem lacking clear objectives			
Research Methodology	• Clear and relevant research methodology with complete implementation				• Clear and relevant research methodology missing few components				• Clear research methodology missing several components				• Inappropriate research methodology				• Lack of clear research methodology			
Analysis of Results & Conclusions	• Excellent analysis of results and complete relevant conclusions				• Good analysis of results missing some minor conclusions				• Normal analysis of results missing some basic conclusions				• Incomplete analysis or results with some conclusions				• Missing proper analysis or results and no conclusions at all			

Assessment Method	LO1	LO2	LO3	LO4	LO5
Project		■	■		

Best wishes

Prof. Ayman Bahaa Eldin and Dr. Islam Tharwat Abdel Halim