MSA University
Faculty of Engineering
ECE Department
Cryptography (ECE 5632)
Project Description

Spring 2024

1 Introduction

In this project, you will be applying your theoretical and practical knowledge of studying modern cryptography. You will be working in a team to implement and test some of the cryptographic tools that are used to secure our information.

You will be working in a team of 3 members. Team members **must** be from the same lab group.

2 Project Description

You are required to implement the Counter with Cipher Block Chaining-Message Authentication Code (CCM) Mode of Operation as described in the NIST Recommendations(click here to download). You should first carefully read and understand its details and usage.
Your implementation **must** satisfy the following:

1. Use Python to implement CCM mode for encryption and decryption. So, your code must consist of at least two functions `encryptCCM()` and `decryptCCM()`.
2. The underlying block cipher to be used in CCM is the AES-128. You must use the `cryptography` python library for AES encryption/decryption. NO OTHER EXTERNAL LIBRARY should be used in your code.
3. Stick to the NIST Recommendations for CCM mode.
4. Verify the correctness of your implemented algorithms by **encrypting** AND **decrypting** each of the ”Example Vectors” given in Appendix (C) in the NIST Recommendations.

3 Deliverables

The following items must be delivered before the discussion day at the announced deadline:

1. Python file(s) containing your implementation and testing code.
2. A report describing your implementation’s flowchart, testing results, and a description of a practical application of CCM mode. Moreover, a detailed description of the work/contribution of each team member in the project should be provided.

4 Grading Scheme

The grade will be individually-based and will be mainly covering the following points:

1. On-time submission of the required deliverables.
2. Correctness and verifiability of the submitted Python code (demo).
3. Originality and format of the submitted report.
4. Responses to questions during discussion.
5. Teamwork.

5 Demo and Discussion

Each team will have at most 15 minutes for making a demo of their implementation and answering questions about their work.

6 Useful Links

- CCM NIST Recommendations: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38c.pdf
- `cryptography` Library: https://cryptography.io/en/latest/hazmat/primitives/symmetric-encryption/

Good Luck!