Project Assignment

Course: Network and Information Security

Fall 2023

Project Description

In this project, you are required to conduct both theoretical and experimental analysis of the five modes of operation for block ciphers defined by NIST. The five modes are electronic code book (ECB), cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB) and counter (CTR). The purpose is to achieve a comprehensive understanding of data encryption with different modes through analyzing and comparing the performance of encryption using the five different modes. Specific tasks include:

(1) Perform theoretical, qualitative analysis of the five modes of operation and conclude your analysis with a ranking of the five modes in terms of overall operational performance.
(2) Implement the five modes of operation for the purpose of experiment.
(3) Conduct experiment using some test data to get performance results and to verify that the results are consistent with those of your theoretical analysis.

Requirements

No specific requirement on the implementation platforms, programming languages or tools that you will use to do the experiment. That is, you are free to use any development environment of your choice. As the outcome of this project, however, you are required to:

(1) implement the five modes of operation for block cipher;
(2) carry out performance evaluation using some test data;
(3) complete a report to present your analysis and experiment results.

Deliverables

(1) Source code of your implementation (soft copy);
(2) A project report (soft copy).

Project Period

Due date: Tuesday, Oct. 24, 2023.

Grading

Theoretical analysis: 20%;
Software implementation and experiment: 40%;
Report writing: 40%.

Warning

Copying someone else’s work is strictly prohibited. If caught, both the offender and the conspirator will need to provide an explanation and, depending on the seriousness of the situation, may be penalized for dishonesty.