CSC 8224 Cryptography

Class Project

1. Project Description

The final project focuses on the implementations and applications of cryptosystems, aiming at understanding their advantages, disadvantages, and cryptanalysis. The ***topics of interests include, but not limited to:***

- Applications of crypto algorithms, i.e., apply existing crypto algorithms to some real-world applications.
- Security analysis of crypto algorithms, including confidentiality, authenticity, integrity, and others, via theoretical analysis or experiment.
- Implementations of attacks, such as analytic attack, side-channel attack, substitution attack, and so on, to break crypto algorithms.

2. Project Requirements

The requirements of the final project are listed as follows:

- ***Project Proposal:*** every group contains ***1-2 students*** and selects a project topic and *report the project proposal, including the project title and participant(s), to iCollege by* ***Mar. 7, 2025***. The collection of project proposal is for presentation scheduling, and the title could be changed before a group's presentation date.

- ***Project Presentation:*** every group should present the project in class ***from Mar. 31 to Apr. 21, 2025***, for which the schedule will be announced by Mar. 15.

- ***Project Report:*** Every group should complete the final project and *submit the project report with source codes and demo by* ***Apr. 25, 2025***. ***No late submission is accepted.***

3. Project Grading Policy

The grade of class project consists of the following two parts:

- ***Project Report (15 points)***, which will be judged in terms of project novelty, project organization, and writing. A complete project report should include abstract, introduction, methodology, experiment, and conclusion, etc. The project report should be written in double column, single space at no smaller than 11pt with maximum page length of 6.

- ***Project Presentation (15 points)***, which will be judged in terms of slides quality, time allocation, response to questions, and speaking, etc.

4. Sample of Project Topics

Some projects in the past years are selected for reference.

- Using Visual Cryptography Technique to Protect Medical Image in Cloud
- Neural Networks in Cryptography
- Voting Using Face Recognition Security System
- Efficient and Secure Model for Access Control in Cloud
- High security keyless home locker/ car garages using Modulo 2 addition algorithms
- Security Analysis of Weakness in RC4 Encryption in Real Life
- Exploitation of Naïve RSA Implementations
- Brute Force Attack on Java's Pseudo-Random Number Generator
- MD5 Collision Attack Implementation and Analysis