Course Project

CE/CZ4010 : Applied Cryptography

Development | **Week 5 to Week 15** | 40% of total marks | Group Activity (maximum 2 students)

In the Development Project, you are expected to design and develop an **Application, Implementation or Demonstration** using basic principles of Applied Cryptography that you learn throughout the course. This a group activity with maximum TWO (2) students per group. You may choose your own "buddy" for the project. Single-member groups are also permitted.

Deliverables and Timeline

This is worth 40% of your total score. Each team must submit the following within the Project Submission Deadline:

Deliverable #1 : 10-minute video presentation of your project, presented by ALL team members.
- Narration on top of slides and demonstration of the final project is sufficient. Face not required.
- Presentation MUST showcase a functional demonstration of your application or implementation.
- Suggestion : Focus more on the development aspects rather than diving deep into mathematics.

Deliverable #2 : GitHub repository for the entire project (excluding hardware components, if any).
- Public GitHub repository with the latest "commit" recorded strictly before the project deadline.
- Private GitHub repository allowed only in special cases, if you need IP protection for "product".
- Suggestion : Focus more on applying cryptography rather than polishing the software and UI/UX.

Deliverable #3 : Detailed README.md on your GitHub repository to "sell" the idea of your project.
- The main README.md file at the root of your repository should describe your project for laymen.
- It should contain brief sections for motivation, research, design, development, use of the code.
- Suggestion : Focus more on the application and usage of your code rather than the core theory.

Timeline **Week 5 : Projects Start | Week 10 : Register your Topic | Week 15 : Submit your Project**

Project Topics

You are free to choose any suitable idea for your project, provided it requires you to put in a decent amount of time and effort in terms of research, design, development and testing of your deliverables. You will find some ideas listed in this document. Feel free to choose one from these or come up with your own idea with a similar level of technical demand.

You MUST check with the TAs or the Instructors about the suitability of your own project ideas before you start working.

Resources

Note that the focus of this project is for you to "use" cryptographic tools and not for you to code everything from scratch, unless you choose a project specifically with the make-it-from-scratch objective. Thus, feel free to use any online library for the cryptographic building blocks. There are plenty, with decent support for all major programming languages.

During the project design and development, if you are confused about the cryptographic building blocks, you may feel free to refer to the lecture/tutorial videos or check out the documentation of the cryptographic libraries you utilize.

Needless to mention, you can always reach out to the TAs and the Instructors at the **Project channel on MS Teams**.

Sample Project Topics

Feel free to choose one from these sample topics or come up with your own idea with a similar level of technical demand. Please check with the TAs or the Instructors about the suitability of your own project ideas before you start working.

Application Track

Primarily focused on design and development of a cryptographic application motivated from some practical use-case.

Topic #1 : Secure File-Sharing platform with untrusted Intermediary

Motivation : Think of Dropbox but without trusting the cloud platform.

- User management module needs to be authenticated to ensure entity authentication and non-repudiation.
- File sharing should follow end-to-end encryption so that the platform does not see unencrypted shared files.
- Confidentiality and Integrity of the shared files must be assured even in case of attacks on the intermediary.

Topic #2 : Anonymous and Secure Grievance Redressal platform

Motivation : Think of NTU Confessions but with redressal accountability.

- Should allow posting of "public issues" on the platform with a notification of issues to relevant authorities.
- Should allow posting of “public redressal” from relevant authorities when the corresponding issue is resolved.
- Anonymous public “validation” of every issue and corresponding redressal based on any suitable mechanism.

Topic #3 : Secure and Accountable “bounties” for Digital Tasks

Motivation : Think of Fiverr but with verifiable accountability of bounties.

- User management module needs to be authenticated to ensure entity authentication and non-repudiation.
- Users can post bounties for certain digital tasks as well as complete tasks posted on the platform for bounty.
- Users can post verifiable “proof-of-delivery” of tasks as well as verifiable “proof-of-payment” upon delivery.

Topic #4 : Secure and Authenticated Password Management Tool

Motivation : Think of 1Password and try to extend upon the basic functions.

- Should support creation of “secure” passwords for different services, as well as maintenance of the passwords.
- Should support updates and extraction of specific passwords based on the requirements of the relevant service.
- Confidentiality and Integrity of passwords should be preserved at all times, in storage, in usage and in transit.

Topic #5 : Secure and Private “intersection” of Sets

Motivation : Grab and Gojek want to identify the drivers who are double-dipping on both platforms while using the same hired vehicle and the same phone number for receiving orders (assuming this behavior is against the individual contracts).

- Parties should be able to computer the intersection of two sets (phone numbers) without disclosing the sets.
- No party should gain any knowledge about sets of other parties (prevent poaching of drivers in the example).
- Every party should gain the knowledge about final intersection set (the common phone numbers are revealed).

Demonstration Track

Primarily focused on design and demonstration of a cryptographic idea motivated from some course-related study.

Topic #6 : Demonstration of WEP Password Cracking

Research : Background study on ARC4 and the attack strategy.

- Capture WEP packets over target WiFi network and analyse the packets exploiting known ARC4 vulnerabilities.
- Crack the password of the target WiFi router using WEP using the analysis on the packets captured in process.

Topic #7 : Demonstration of attacks on SPN Ciphers

Research : Background study on Linear/Differential Cryptanalysis.

- Implement a reduced-size simple SPN block cipher and mount Linear or Differential Cryptanalysis on the same.
- Recover the key of the reduced-size simple SPN cipher key using the Linear or Differential analysis techniques.

Topic #8 : Demonstration of attacks on "weak" RSA

Research : Background study on RSA Cryptanalysis/Attacks.

- Implement a simple but practical RSA-based protocol that is known to have a "weak" implementation of RSA.
- Demonstrate an attack on the protocol exploiting the "weak" RSA implementation to recover key or plaintext.

Topic #9 : Hardware Implementation of Randomness

Research : Background study on Hardware TRNGs and PRNGs.

- Implement a TRNG or a PRNG circuit on hardware from scratch, using simple digital components and circuits.
- Generate sufficiently many random bits using the circuit (in MBs) so that they PASS all NIST Statistical Tests.

Topic #10 : Implementation of a Certification Authority

Research : Background study on Signatures and Certificates

- Should support Certification and Revocation of submitted Public Keys, and API for Certificate Verification.
- Should support hierarchical Certificate Issue and Revocation, and Key Generation if the parties ask for it.

Assessment Criteria

Members in a two-student group will have to specify "individual contributions" while submitting the project deliverables. While the group will be evaluated as a whole, if individuals make disproportionate contributions, the Instructors may discuss such issues with the group and use this factor to calibrate personalized bonus/penalties within the same group.

Fail (0-40%) : Minimal set of expectations not achieved.

Pass (41-74%) : Minimal requirements achieved. However, the project lacks some or several of ingenuity, novelty, level of complexity, validation, or the presentation and reporting on the end-product is mediocre.

High (75-100%) : The project exhibits ingenuity, novelty and a good level of complexity, results are well validated, and the presentation and reporting on the end-product is well done.