Nova Southeastern University
College of Computing and Engineering
ISEC 620 Applied Cryptography
Fall 2020
(August 17 – December 6, 2020)
Course Project
Due Date: November 15, 2020 (firm)
Instructor: Dr. Junping Sun

In this assignment, you will be expected to select and study a specific topic in one area of applied cryptography and its applications to areas of computer security, to do a comprehensive literature search and survey, and to write a technical paper on the selected topic by yourself. The technical paper that you are asked to write can be a detailed comprehensive survey on some specific topic or the *original* research work which will be done by yourself.

Requirements and Instructions for the Written Project Report:

1. The objective of the paper should be very clear about subject, scope, domain, and the goals to be achieved.

2. The paper should address the advanced and critical issues in a specific area of applied cryptography and its applications to areas of computer security. Your research paper should emphasize not only breadth of coverage, but also depth of coverage in the *specific* area.

3. From the systematic study point of view, you may want to read a list of technical papers from relevant magazines, conference proceedings, journals, theses, and dissertations in the area of the topic you choose. It might be beneficial to review or to browse about 5 to 10 closely relevant technical articles before you make your decision on the topic of this research project.

4. The research paper should reflect the quality at certain academic research level.

5. The length of this paper should be about at least 25 to 30 pages (about 3000-3500 words) in double space.

6. The research paper should include adequate and appropriate abstraction or introduction, and reference list.

7. The research paper should be methodology and/or problem solving oriented, so it should define the problem under discussion clearly, and present/illustrate/elaborate the methodology for the underlying problem solving as clearly as possible.

8. The research paper should give the measurable conclusions and future research directions (this is your contribution).

9. From pedagogical perspective, you might want to use examples, diagrams, pictures, etc. to help explain and illustrate some concepts, definitions, principles, mechanisms, algorithms/methodologies.

10. Please write your paper in your **own words and statements**, and please give the names of references, citations, and resources of reference materials if you want to use the statements from these reference articles.

11. For the format and style of your research paper, please make reference to the Publication Manual of the American Psychological Association, the style and format of ACM/IEEE journals, and/or CEC Dissertation Guide.

12. For the project report, please attach your signed authorship certificate page. **Please include your name, your NSU email usercode, your NSU ID, and your contact phone number on the title page of your paper submission.**

13. Please post the abstract of your written project in the discussion, so every one could the information with the class. (If any one is interested in your project, he/she could request a copy from you after the submission.)

Suggested Topics in Cryptography, But Not Limited

Anonymity and Privacy
Broadcast encryption and traitor tracing
Computer architectures for public-key c and secret-key cryptosystems
Cryptoanalysis
Cryptography applications
Cryptographic protocols
Cryptographic processors and co-processors
Digital signature
Encryption standards
Efficient cryptographic algorithms
Foundations of cryptology (e.g., from computational number theory, complexity theory, combinatorics)
Implementation of cryptosystems and their integration into secure systems
Message Authentication
Modes of operation (e.g., Authenticated encryption and signcryption)
Distributed cryptography)
Network and Web security
Public-key cryptosystems and hash functions
Quantum Cryptography
Reconfigurable computing in cryptography
Secure cryptographic algorithms
Secret-key cryptosystems and hash functions
Secure operating systems and trusted computing
Special-purpose hardware for cryptanalysis
Various applications of cryptography
Voting system security

Reference Magazines:

Communications of ACM
IEEE Cloud Computing
IEEE Computer
IEEE Intelligent Systems
IEEE Internet Computing
IEEE Pervasive Computing

IEEE Security and Privacy
IEEE Software

Reference Journals:

ACM Computing Surveys
ACM Computing Reviews

ACM Transactions on Computing Systems/TOCS
ACM Transactions on Information and System Security/TISSEC

Computer and Security
Cryptologia
IBM Systems Journal

IEEE Transactions on Big Data
IEEE Transactions on Computers
IEEE Transactions on Dependable and Secure Computing
IEEE Transactions on Service Computing
Information System Security
International Journal of Digital Libraries
International Journal of Information Security
International Journal of Network Security
Journal of Computer and Network Security
Journal of Computer Security
Journal of Cryptology
Network Security Journal

Proceedings:

Proceedings of ACM Conference on Computer and Communication Security (ACCS)(Since 1993)
Proceedings of ACM Symposium on Access Control Models and Technologies (SACMAT) (Since 1995)
-Previously ACM Workshop on Role-Based Access Control (RBAC), 1995-2000
Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS) (Since 2006)
Proceedings of Annual Computer Security Applications Conference (Since 1985)

Proceedings of Annual International Cryptology Conference
Proceedings of European Cryptology Conference

Proceedings of IEEE Information Assurance Workshop (Since 1999)
Proceedings of IEEE Symposium on Security and Privacy (Since 1980)
Proceedings of IEEE Computer Security Foundations Workshop (Since 1987)
Proceedings of International Cryptology Conference
Proceedings of International Conference on the Theory and Application of Cryptology and Information Security
Proceedings of IFIP International Information Security Conference

News Letters:

Cipher (Electronic Newsletter of the Technical Committee on Security and Privacy, A Technical Committee of the Computer Society of IEEE)

Useful URLs:

http://www.acm.org
http://www.compuer.org
http://www.ieee.org
http://www.acsac.org

Sample Format of Project Report

1. Title Page

In general, the number of words in the title of report should be limited around 10 words if possible. **The title page should have your name, email, contact information, and term date below the paper title.**

2. Abstract

The abstract page should summarize the highlight of your project to tell the audience what have been done in the research project.

3. Table of Contents

The TOC part should list all titles of sections and subsections with page numbers.

4. Introduction

This part introduces the audience with necessary information to guide them into the subjects of your research project.

5. Background and Literature Review

6. Statement of the Proposed Research or Study

With the discussion in Background and Literature Review, the proposed research and study can be given in the format of, possibly, Problem Statement to indicate what to be studied, investigated, researched, and/or achieved from this project.

7. Methodology

Based on the Problem Statement and the objective to be achieved, you may want to elaborate the underline methodology to be used in order to fulfill the research task and achieve the goal of the research/study. If possible, please provide elaboration of rationales in both depth and width.
It is better to use illustrative examples to explain the methodology employed in this project.

8. Experiment Design and Result Analysis

Provide the details of how experiments are designed and conducted, and observation from the experiment. Analysis of experimental results are important based on your observation, understanding, interpretation, etc. with some performance analysis methods.

9. Conclusion

Summarize your research/study by giving some conclusion from the project, and may provide future research/study directions with discussion of potentials.

10. Reference List

11. Appendix (if necessary)

For style, please make reference APA Manual, ACM, IEEE publications, CEC Dissertation Guide.

Certification of Authorship

Submitted to (Advisor's Name):

Student's Name:

Date of Submission:

Purpose and Title of Submission:

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature:_____