Singapore Polytechnic
School of Computing

ASSIGNMENT ONE

INTRODUCTION

This assignment constitutes part of your in-course assessment (20%) as mentioned in the module overview. It is important that you allocate sufficient time to complete this assignment.

OBJECTIVE

The learning objective of this assignment is to research into the assigned topic and to make a presentation of what you have gathered to the class. The team will be tasked to:

- Conduct a simple research on the chosen topic;
- Conduct a student-led presentation. These include organizing the topic presentation, managing the Q & A and Quiz session, etc.;
- The whole duration of the presentation **should not be more than 40 minutes.**

The student-led presentation is aimed at studying the assigned topic in depth which is related to the Applied Cryptography in the real world.

INSTRUCTIONS

1. Students are to complete the assignment in groups of (up to) 4 members.
2. The presentation slides, and tailor-made demonstration programs if any, are to be submitted to Blackboard before the start of the presentation.
3. The student-led presentations will be in ACG classes of week 4 to week 6.
4. Read the following sections for the presentation requirements

PRESENTATION REQUIREMENTS

1. The duration of the presentation is 40 minutes for each group. All members must participate in the presentation.
2. Your team will present the topic to your fellow-classmates during the practical sessions. The main purpose is to share and educate your fellow classmates on the main points of your research topic.
3. The team needs to manage the Q & A and Quiz session (at least 5 mins) properly.
4. There should be at least 5 questions for the quiz. The assessment is meant to reinforce what have been shared during the presentation.
5. Students who ask question(s) during the seminar will be given participation marks under general performance.

6. References:
    a. Please quote the reference if you use any materials in your presentation slides, please quote the reference.
    b. Please acknowledge the source when you refer to books, journals, or online resources.

ASSESSMENT CRITERIA

The presentation will be assessed as follows:

Group score

- Technical contents – overview and technical contents. (20 marks)
- Presentation – clarity and presentation skills (20 marks)
- Novelty (video clip [original], skit, experiment, demo program, etc) (10 marks)
- Applications – using real world examples. (10 marks)
- Relevance and completeness to the topic. (10 marks)
- Q & A and Quiz sessions –management of the session. (15 marks)

Individual Score

- Application, knowledge and comprehension. (15 marks)

POSSIBLE TOPICS

1. How can we encrypt and sign Office and PDF documents? Is it safe and useful?
2. How can we decrypt a zip archive without knowing the password?
3. How does blockchain encryption work? Is it safe and useful?
4. How is data integrity protected in cloud computing? Do they use strong cipher?
5. How Key exchange strategies are used in network communications
6. How cryptography is used in web browsers to protect its users.
7. How cryptography is used to protect email users.
8. How does contactless NFC card work? How is it protected?
9. How is credit card purchase protected?
10. How popular hashing functions works? Are there known weaknesses?
11. A review on cryptanalysis tools.
12. A review on AES standard and its weakness.
11. A review on steganography tools. How data could be hidden (and rediscovered)?
12. A review on encryption methods used in Internet of Things (IoT).

13. A review on methods used to store user credentials and data on popular operating systems. (Working principles, weakness).
14. A review in privacy enhancing technologies

You are free to propose other Applied Cryptography related topics that are not listed above. Please approach your lecturer for consultation and confirmation on your newly proposed topic for the presentation.

- The team is recommended to use the textbook as the main guide, and also to include other journals and/or reference materials for your presentation.

- The team is strongly encouraged to check with the instructor on your research topic, review of presentation slides, the presentation coverage, completeness of research, etc.

LATE SUBMISSION

Submission Date/Time: 8rd Nov 2021 / 6 pm. (via Blackboard)

50% of the marks will be deducted for assignments that are received within ONE (1) calendar day after the submission deadline. No marks will be given thereafter.

Exceptions to this policy will be given to students with valid LOA on medical or compassionate grounds. Students in such cases will need to inform the lecturer as soon as reasonably possible.

Students are not to assume on their own that their deadline has been extended.

Marks awarded for the presentations will be equally divided for the parties involved.

Warning: **plagiarism** – any group found plagiarizing in this assignment would be ***penalized***. Marks awarded for the report will be equally divided for the parties involved.

~ End of the Assignment Specification ~