



UTM
UNIVERSITI TEKNOLOGI MALAYSIA

**INTERNATIONAL JOURNAL OF
INNOVATIVE COMPUTING**

ISSN 2180-4370

Journal Homepage : <https://ijic.utm.my/>

Case Study and Cooperative Learning in Cryptography Course

Nazrin Amirul Neu Jan Tan @ Atan & Rashidah Kadir
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia

Submitted: 14/09/2020. Revised edition: 19/10/2020. Accepted: 21/10/2020. Published online: 19/11/2020
DOI: <https://doi.org/10.11113/ijic.v10n2.276>

Abstract—Cryptography is one of the important components in data and telecommunications, it is important when communicating over any entrusted medium, which includes just about any network, particularly the Internet. It is also one of the important courses in Information Technology courses. For now, students seem to be hard to understand because they are lack of interest in learning this course. This problem is caused by their awareness towards the application and the usage of cryptography. In this study, a different approach will be used to open the students' eyes towards the importance cryptography and the usage of cryptography application in their daily life to increase their interest in cryptography along with their understandings in cryptography. This study will focus on an approach that will improve the teaching interest and their understanding of the student by using case study and student-centered learning approach which is the cooperative learning approach. A case study is developed to carry out the tasks that will make the students realized the importance of cryptography. In order to make sure that the students' get better understanding towards cryptography, the cooperative learning practice will be implemented. At the end of this study, the result from the implementation of the case study and cooperative learning will be analyzed and evaluated. The tasks of the cooperative learning practice will be identified in this study and the effectiveness of the practice will be measure based on the tasks given. Finally, the effectiveness will be evaluated after the given tasks is finished. This evaluation will be the final result of this study whether the implementation of case study and cooperative learning practice is effective than traditional teaching method or vice versa.

Keywords—Cryptography, student-centered, cooperative learning, teaching method

I. INTRODUCTION

Cryptography was a Greek word for "secret writing." It has a long history going back for many years. Professionals make

a separation between ciphers and codes. A cipher is a character-by-character or bit-by-bit transformation. In comparison, a code changes one word with another word or symbol. Cryptography is the science of writing in secret code and it is widespread in development of computer communications. Cryptography is not only used to protect data from being modified, but can also be used for user authentication. In general, three types of cryptographic schemes usually used to achieve these goals which is symmetric cryptography, asymmetric cryptography and Hash functions.

Cooperative learning is one of the teaching methods that the new curriculum reform campaign for. This learning approach was once described as "most important and successful teaching method reform in the last decade." Some research has been done on cooperative learning and based on the research, it discovers that cooperative learning enables student to get benefits to exchange idea when they are solving complex problem and giving them a better problem-solving skill. Besides, cooperative learning enabling the student involvement to communication and helps to develop the individual's views in problems solving.

In addressing the challenges in Cryptography course, a new approach of teaching and learning must be considered for increasing the interest of student and better understanding for this course. Currently, one of the problems encountered is teaching method and the environment. This research will focus on an approach that will improve the teaching environment and the understanding of the student by using student centered learning approach.

II. CHALLENGES OF CRYPTOGRAPHY TEACHING AND LEARNING

To be a better Computer Science or Computer Information System students and other information technology expertise, better understanding of Cryptography is a must nowadays.

Lonsdale *et al.* [1] stated that some of the computing university students having hard times in learning Cryptography because there is not enough prerequisite proficiency and not able to implement the concepts using their programming skill set.

Gondi *et al.* [2] finds that one of the major issues in Cryptography course is the complexity of the mathematics used in encryption. He stated that one of the topics in Cryptography course which is the Public Key Cryptography concept will require the students to use the high-level mathematical skill. He also finds out that the traditional approach on teaching Cryptography is not effective.

In reality today, students finding it is hard to learn Cryptography and one of the causes are the method of teaching and learning the Cryptography itself. In order to get a better result in teaching and learning Cryptography, a new approach of teaching and learning need to be conducted instead of using the traditional teaching and learning approach to encourage students to get familiar with Cryptography algorithm and let the students understand the application of Cryptography.

Even though Cryptography is important and will be a good use for the future of the students, there are challenges that are needed to be overcome when it comes to this course. The challenges are as the follows:

A. *Student found it is hard to learn and practice Cryptography algorithm.*

This is because in Cryptography there is many algorithms that are complicated and is deep theories required to be understood in order to understand the algorithm itself. According Hu *et al.* [3], this may lessen the students' progresses in learning the cryptography algorithms.

B. *Students need a high-level mathematical skills*

Gondi *et al.* also [2] stated one of the major issues in Cryptography is the complexity of the mathematics used in encryption. The traditional approach is not very effective in teaching a course that are required the high-level mathematical skills since it also need a student who master the mathematical skills to make cryptography easier.

C. *Insufficient number of class hour*

Adamovic *et al.* [4] stated that Cryptography are related to many other subjects that are related sciences like mathematics, communications and computer science. It is not enough if this

course is threatened as the same as the other course which only took around 48 hours per semester.

D. *Students lack of experimental work*

According to Adamovic *et al.* [4], the lack of the constructive application of cryptography is the main causes that let the students less interested in cryptography course.

III. STUDENT-CENTERED LEARNING APPROACH

A number of studies has been selected to discuss on the effectiveness of a teaching method to student. In this study, the chosen learning and teaching approach is student-centered learning approach which is one of the most used teaching and learning approach nowadays. There are many types of student-centered learning and teaching approach like Active Learning and Cooperative Learning but this study will focus on one type of the approach which is Cooperative Learning approach.

Emaliana [5] carried a study to investigate English Department student learning needs involving their attitudes against student-centered and traditional teaching method. The result of this study, she found out that this research provides the teachers with many useful information on students' learning requirements as an input to material planning and classroom instruction practice. This study also demonstrates the importance of a good understanding of the students. The other findings of this study also proved that both teacher-centered and student-centered learning should be implemented together to improve the teaching and learning process.

Gutman *et al.* [6] done a research the impact of Student-Centered Learning technologies on professional Development. He stated that the modern educational technologies may lead to the effective organization. The result that they found that the student-centered learning approach is very effective in developing the that personality-activity character and a few advantages that can make them fundamental to reach the quality of education in various disciplines.

A. *Active Learning*

According to Demirci [7], active learning allows students to give attention on creating knowledge with an emphasis on skills that develop students' way of thinking because of the students' active impact and involvement in the learning process. He done an experiment on two similar classes and he find out that there is significant difference between both classes at the end of the experiment. The classes is divide into two which is active learning class and traditional learning class. The result showed that active learning approach is significantly better than traditional approach both in students' scores and attitude.

B. *Cooperative Learning*

Anderson [8] write two cooperative learning's principles as the following:

this tasks is also to determine the result between different teaching approaches.

a) Principles of Cooperative Learning

i. Positive interdependence - For activity that really need cooperative skills because the group members must work as a team to achieve their goal and not in competition with each other, so that they fail or success together as a team.

ii. Individual accountability - The success of the group is depending on the contributions of all group members which making each of them accountable for both of their own learning and contributions to the group as they need to. He also stated that as the cooperative learning approach is widely spread nowadays, it also faces the challenge of adapting the teaching technique in large classes of young learners. The challenges are stated as the following:

- i. Differentiation in large mixed-ability classes.
- ii. Preventing certain learners from dominating in group work.
- iii. Encouraging communication when exams are knowledge-focused.

IV. RESEARCH FRAMEWORK

In this study, a research framework is developed as a guidance to carried out this experiment and helps to ensure this experiment is on the right track. This framework also provides supports for carrying out the activity for this study and make sure that this study can be done within the expected time (Fig. 1).

V. PHASE DESCRIPTION

A. Phase 1: Planning

At the beginning of this research started with the study of Cryptography teaching and learning. The objectives of this research are to identify and plan the tasks that are needed to carry out for cooperative learning practice in cryptography course, to measure the effectiveness of cooperative learning practice in cryptography course based on the tasks that will be given to the students, and to evaluate the effectiveness of cooperative learning in cryptography course based on the task given. In this phase, it will focus on review and study the on the related existing research.

B. Phase 2: Design Implementation

During this phase the tasks for cooperative learning practice is designed and developed. After the tasks is revised, it will be conduct in the class. To measure the effectiveness of the cooperative learning approach, there will two different types of teaching will be applied to two different classes. One of class will apply cooperative learning practice while the other using the traditional teaching approach. The purpose of

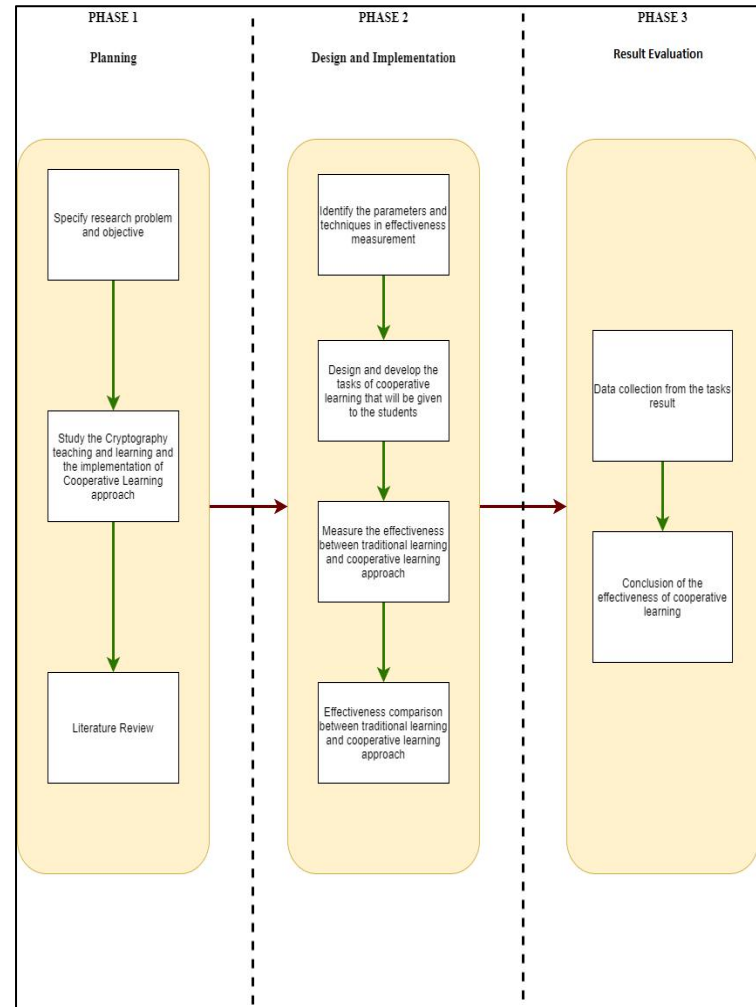


Fig. 1. The framework of Case Study and Cooperative Learning Practice in Cryptography Course

C. Phase 3: Result Evaluation

This phase is the final phase of this research where the result of this study will be summarised. The data collection of the tasks given to the students will be evaluate and analyse. From this phase, the effectiveness of the cooperative will be determined based the result of the tasks.

VI. PROPOSED SOLUTION

In this study, a class consist of 80 students who is taking Cryptography course will be divided into two section in semester 1 session 2020/2021. Each section will be using a different teaching and learning approach. On one section, the traditional teaching approach while another section will implement cooperative learning approach. The section that implementing the cooperative learning will be given tasks that

are specially design for this study while the other section not. During this experiment, the class that implement the cooperative learning practice will carried out the tasks given based on the case study that has been developed. For the completing the tasks, the cooperative learning practice will be implemented to the students. The students also will be given an assessment before and after the finished the tasks in order to measure the level of knowledge and their understandings in cryptography. The result from this experiment will be compared with the other class that are not implemented cooperative learning in the class.

VII. ACKNOWLEDGMENT

In preparing this research, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Madam Rashidah Binti Kadir, for encouragement, guidance, critics and friendship. She also gives guidance, advices and motivation. Without her continued support and interest, this thesis would not have been the same as presented here.

I am also indebted to Universiti Teknologi Malaysia (UTM) for funding my MSc study through Encouragement Research Grant. Librarians at UTM also deserve special thanks for their assistance in supplying the relevant literatures.

My fellow postgraduate student should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at

various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family member especially my mother for always supporting me for all the time during finishing this research.

REFERENCES

- [1] Lonsdale, C., Buckland, R., & Wen, R. (2018). Unconventional Cryptography. *Phil. Trans. Roy. Soc. London*, A247, 529-551, April 1955.
- [2] Gondi, V., Hua, D., & Bajracharya, B. (2019). Engaging Students in Learning Public Key Cryptography. *CTE Journal*, 7(2).
- [3] Hu, Y., & Willis, R. (2016). A Framework for Developing Visualization Tools for Learning Cryptography Algorithms from Hampton University. http://science.hamptonu.edu/compsci/docs/hu_p7.pdf, Retrieved September, 23.
- [4] Adamovic, S., Sarac, M., Stamenkovic, D., & Radovanovic, D. (2018). The Importance of the Using Software Tools for Learning Modern Cryptography. *Int. J. Eng. Educ.*, 34(1), 256-262.
- [5] Emaliana, I. (2017). Teacher-Centered or Student-centered Learning Approach to Promote Learning? *Jurnal Sosial Humaniora*, 10(2), 59-70.
- [6] Gutman, E. V., Gilyazova, K. R., & Karakozov, S. D. (2019). The Impact of Student-centered Learning Technologies on Professional Development. *Int J Edu Sci*, 27(1-3), 89-96.
- [7] Demirci, C. (2017). The Effect of Active Learning Approach on Attitudes of 7th Grade Students. *International Journal of Instruction*, 10(4), 129-144.
- [8] Anderson, J. (2019). Cooperative Learning: Principles and Practice. *English Teaching Professional*, 121, 4-6.