Exploration of Heuristic Teaching in the "Information and Network Security" Course Based on the OBE Concept

Zhimeng Liu

School of Computer Science and Technology, Shandong Technology and Business University, Yantai Shandong, 264005, China

Abstract. In the "Information and Network Security" course, cryptographic techniques pose challenges as they involve extensive mathematical knowledge that is complex and hard to comprehend. Additionally, during the traditional teaching process, the basic knowledge of cryptographic mathematics and the application of cryptographic techniques are often taught separately, leading to suboptimal teaching outcomes and low student learning initiative. This research group proposes an OBE - oriented modular and guided teaching mode, integrating lectures and practices and leveraging an online course management platform. The aim is to enhance students' enthusiasm for autonomous learning and improve the overall teaching effectiveness of the course, considering the relationships and coherence among knowledge points in each chapter.

Keywords: Applied Undergraduate Education; Information and Network Security; Heuristic; Online Teaching Management Platform.

1. Introduction

The rise and widespread adoption of the Internet, especially the in - depth integration and application - empowered development of new IT technologies such as the Internet of Things, artificial intelligence, and blockchain, have had a far - reaching impact on human society. While the Internet of Everything brings convenience to people's lives and work, it also introduces unprecedented security risks. General Secretary Xi Jinping has emphasized on multiple occasions that "without cyber security, there is no national security" and pointed out that technology is a "double - edged sword." It can benefit society and the public on one hand, but on the other hand, it may be exploited by some individuals to undermine public and people's interests [1]. In response to the new situation and changes in cyber security, the Party Central Committee and the State Council attach great importance to information security disciplines, professional construction, and talent cultivation. They have made a series of crucial strategic arrangements regarding the construction of a cyber security talent team [2]. Currently, although China's cyber security talent team has achieved significant phased progress, there are still prominent issues, such as an overall shortage of cyber security talents, which cannot meet the demands of social development for such professionals.

As an applied undergraduate institution, Shandong Technology and Business University has incorporated cyber security - related directions into majors like network engineering and computer science and technology since 2016. It has also offered courses such as "Information and Network Security" to strengthen students' knowledge in cyberspace security [3].

2. Current Teaching Situation of the Information and Network Security Course

As a core course in network engineering, "Information and Network Security" consists of theoretical and practical teaching components, with 48 hours of theoretical courses and 16 hours of practical courses, totaling 64 hours. The teaching content encompasses the fundamentals of cyber security, the basics of cryptography, and the specific applications of cryptography in network environments. In- class teaching mainly covers classic cryptographic primitives, including encryption algorithms, message digests, authentication codes, signature technology, and key exchange. The objective is to enable students to establish the basic concepts, models, and ideas of confidential communication, data integrity inspection, source authentication, and key exchange based on cryptographic mathematics, and to select appropriate security mechanisms to ultimately establish an

information security system and provide security services for the system. The cyber security technology and application part focuses on designing security schemes using classic cryptographic primitives in network environments to achieve desired security goals.

However, due to the high comprehensiveness of the curriculum, which involves multiple disciplines such as computer science, network technology, communication technology, cryptography, and mathematics, students face challenges in learning. The difficulties encountered in traditional teaching are as follows:

1) The secure communication model in the basic part of cryptography requires a solid foundation in number theory and abstract algebra. However, the content covered in the first - year "Discrete Mathematics" course is insufficient, lacking essential cryptographic mathematics knowledge such as first - order congruence, Euler's theorem, Fermat's little theorem, the Chinese Remainder Theorem, groups, rings, and fields. Given the extensive teaching content, limited class hours, and high difficulty level, it is necessary to appropriately increase the teaching hours dedicated to the basic part of cryptography.

2) In traditional sequential teaching, the teaching process follows the textbook chapters. Due to the wide - ranging mathematical knowledge required for this course, the knowledge points are relatively scattered, and there is weak connectivity between different parts. This makes it difficult for beginners to understand, increasing the learning difficulty for students and resulting in an incomplete grasp of knowledge. Therefore, it is necessary to reconstruct the textbook chapters from the perspective of implementing cryptographic algorithms based on the requirements of cryptographic primitives and integrate the cryptographic mathematics foundation into the cryptographic algorithm implementation chapter to enhance the relevance between the foundation and application.

3) The traditional teaching mode has a relatively simplistic teaching approach, typically relying on the combination of PPT and blackboard writing. This method leads to passive learning among students, insufficient teacher - student interaction, and the inability to promptly monitor students' understanding of knowledge points. An online teaching management platform can be utilized to enhance teaching interaction and monitor students' knowledge acquisition through chapter - based tests.

To improve the teaching effectiveness and students' learning autonomy, the course team has drawn on the successful teaching experiences of other institutions. By integrating the online platform "Classroom Pie" to manage the course teaching process, the team explores a new heuristic teaching model of "lecture - practice - test - evaluation." This model modularizes and casifies theoretical knowledge, increases teacher - student interaction, and combines teaching with practice.

3. Teaching Exploration and Practice

OBE (Outcome - Based Education) is centered around learning outcomes, emphasizing the development of students' abilities, knowledge, skills, and values through learning [5]. Learning outcomes are the core of the OBE concept, and they serve as the primary criterion for evaluating teaching quality and learning effectiveness [6]. Shandong Technology and Business University, as an applied undergraduate college, conducts professional generalist education with an application - oriented focus. It emphasizes the systematic and solid acquisition of basic theoretical knowledge [3], regards the cultivation of system engineering capabilities as the foundation of education, and promotes the integration of academic education and professional literacy.

To further enhance the teaching effect and strengthen students' understanding and mastery of the course content, the research group has learned from advanced educational concepts, methods, and teaching practices of domestic and foreign universities. Combining with the actual situation of the network engineering professional training program, the group actively explores a new teaching model. This model is based on the "Classroom Pie" classroom management platform, features heuristic

teaching, and integrates online and offline lectures and practices. The goal is to continuously optimize teaching methods and improve teaching quality through new teaching reforms.

3.1 Exploration and Practice of Modular Teaching

Modular teaching involves dividing classroom teaching content according to the independence and relevance of each knowledge point in the course. This results in relatively independent basic knowledge units that are easier for students to learn and master, aiming to stimulate students' enthusiasm for course learning by making learning more accessible and engaging [3].

The teaching content of cryptography basics includes classical symmetric cryptographic algorithms (such as substitution ciphers), modern symmetric cryptographic algorithms (such as DES and AES), asymmetric cryptographic algorithms (such as RSA, Elgamal, and ECC), message digests, message authentication codes, and digital signature algorithms. Since the cryptographic basics and cryptographic mathematics knowledge required for specific cryptographic technologies in each chapter are relatively independent, modular teaching is highly suitable. Thus, the course team uses a top - down approach to divide the course content into knowledge modules, as presented in Table 1.

Table 1. Distribution of Basic Knowledge of Cryptography Mathematics

<table>
<tr><th>Mathematical Fundamentals of Cryptography</th><th>Traditional Cryptography</th><th>Modern Symmetric Cryptography</th><th>Asymmetric Cryptography</th><th>Cryptography Applications</th></tr>
<tr><td>Modulo Operation</td><td>substitution cryptography</td><td rowspan="3">DES
IDEA
AES</td><td rowspan="2">RSA
ElGamal
ECC</td><td rowspan="6">hash function
MAC
Digital signature
digital certificate
Authentication and
Key Management</td></tr>
<tr><td>Congruence</td><td></td></tr>
<tr><td></td><td>permutation cryptography</td><td></td></tr>
<tr><td>Group</td><td></td><td rowspan="3">AES</td><td>ElGamal, ECC</td></tr>
<tr><td>Ring</td><td></td><td rowspan="2">ECC</td></tr>
<tr><td>Field</td><td></td></tr>
</table>

In order to fully illustrate the connections between knowledge points in each section and their roles in implementing cryptographic algorithms, the research group adopted a bottom - up approach in teaching design. This approach clearly integrates relevant knowledge points into composite knowledge units. During classroom teaching, these inter-related yet independent complex knowledge points are combined to design comprehensive classroom teaching cases. Taking the Elgamal digital signature as an example, the mathematical knowledge involved in implementing the algorithm is shown in Figure 1,

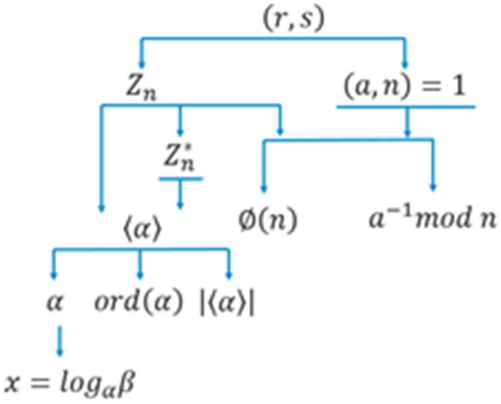

Figure 1. Elgamal digital signature knowledge point association diagram

including the following concepts: Z_n, Z_n^*, $(a,n)=1$, Euler function $\emptyset(n)$, multiplicative inverse $e^{-1} mod\ p$, cyclic group $\langle\alpha\rangle$, discrete logarithm problem $x = log_\alpha \beta$) etc.

3.2 Exploration and Practice of Course Cases Combining Speech and Practice

The research group adopts a heuristic teaching method that first imparts theoretical knowledge and then encourages practical application. In the "lecture - practice - test - evaluation" teaching model, "lecture" refers to determining the teaching content for a class according to the teaching plan. Through various organizational forms, following teaching principles, highlighting key points, and addressing difficult concepts, the instructor provides comprehensive explanations to help students achieve basic learning goals, quickly master knowledge, and enhance their capabilities. "Practice" is conducted in a manner that combines online - based activities as the main approach, supplemented by offline tasks, and extended to after - class activities. After in - depth lectures on major knowledge points, online "practice" is often used to test students' understanding of minor knowledge points, allowing for appropriate control of the teaching pace. Offline activities focus on examining comprehensive knowledge modules and the entire knowledge section, enabling students to identify and fill in knowledge gaps.In the teaching of the Elgamal digital signature, the teaching process starts with real - life signatures. Students are guided to understand the functions and characteristics of handwritten signatures. Then, taking the scenario of Bob receiving a message containing Alice's identity in a network environment as an example, students explore how Bob can authenticate the message's origin from Alice, which helps them understand the necessity and implementation process of digital signatures as a substitute for handwritten signatures.

To fully integrate lectures and practices, the teaching design uses the form of classroom - sent interactive courseware + interactive answers + section tests to teach the principles and functions of signatures, the composition and functions of digital signatures, and the implementation of the Elgamal signature and verification algorithms. The PPT provides a knowledge framework for students to grasp the algorithm structure comprehensively. The interactive answering function of "A$^+$ Classroom Pie" is used to test students' understanding of the prerequisite knowledge for implementing the algorithm. The answering time can be set according to the complexity of the knowledge points (for example, 2 minutes). The test question analysis function of "A$^+$ Classroom Pie" enables teachers to quickly understand students' knowledge acquisition and decide whether to reinforce the explanation of certain knowledge based on the analysis results, as shown in Figure 2.

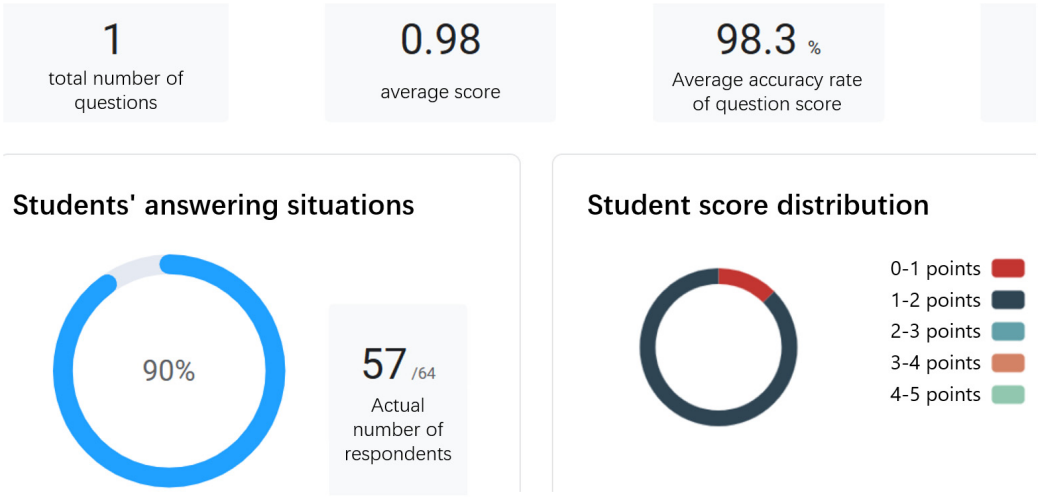

Figure 2. Schematic Diagram of "Classroom School" Test Question Analysis

4. Exploration and Practice of Assessment Methods

"A$^+$ Classroom Pie" is an efficient online teaching management platform that provides interactive classroom teaching, online live teaching, and mixed teaching whole process management in line with users' habits. At the end of each unit lecture, the "test" module is used to conduct unit tests to evaluate students' knowledge acquisition. Subsequently, knowledge points with frequent errors are reviewed,

and the relationships between knowledge points are clarified. This further enhances students' understanding and mastery of knowledge and improves the teaching effect, as shown in Figure 3.

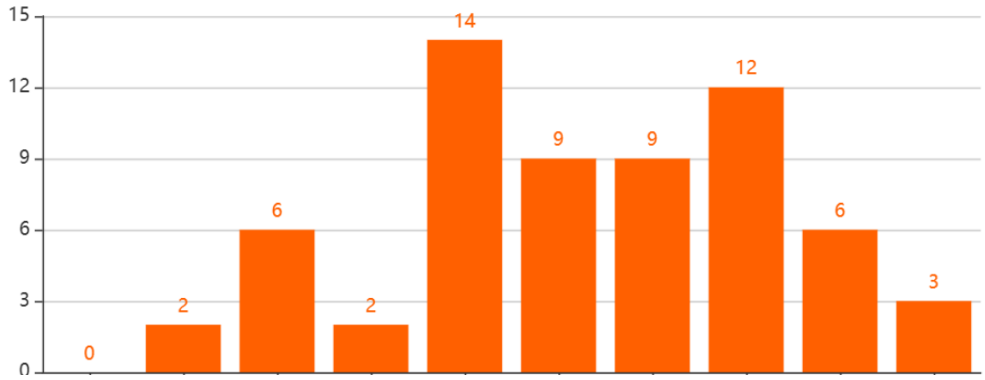

Figure 3. Example Diagram of Online Test Statistics Combined with Lecture and Practice

So far, the research team has completed the decomposition of cryptographic technology knowledge points based on Classroom Pie. The functions of online lesson planning, online homework, and online testing have been realized, enabling the comprehensive management of online and offline teaching scenarios before, during, and after class. This also facilitates the implementation of flipped classroom teaching after class and promotes students' enthusiasm for independent learning.

5. Summary

To implement the student - centered and result - oriented OBE engineering certification concept, adapt to the new situation of higher education popularization and the growing demand for applied engineering talents in society, and improve the teaching effectiveness of the "Information and Network Security" course, this paper proposes a case - based teaching method using an online platform - based classroom management platform. The teaching content is organized in a top - down manner, the teaching process is designed based on knowledge modules in a bottom - up fashion, and enhanced teaching interaction is used to achieve a teaching effect where students are eager and able to participate. Teaching practice shows that this teaching method can boost students' learning initiative, address the drawbacks of traditional teaching methods, and improve the overall teaching quality of the course.

Acknowledgments

The author expresses gratitude to the editor and reviewers for their valuable suggestions. This work is supported by Shandong Business School Teaching Research Project(No. S201146), and Shandong Province Education and Teaching Research Project (No. 2021JXY037).

References

[1] X. Yang. Analysis of big data development in the perspective of national security [J]. National Governance, 2016, (37): 41-48.

[2] Y. Wang, N. Kang, R. Zhang. CISP promotes the rapid development of cyber security talent work [J]. China Information Security, 2023 (06):13-18.

[3] Z. Liu, Y. Zhao. Lecturing and teaching reform exploration of "computer cyber security" course [J]. Modern Computer, 2019, (12): 76-78.

[4] J. Sun, D. Fu. Exploration and practice of teaching method of "Cryptography" course [J]. Information cyber security, 2009, (07): 65-67.

[5] R. Feng, B. Li, L. Zhang. Research on the cultivation of master's talents in landscape architecture based on the strategic needs of OBE concept rural revitalization - a case study of Jiangxi Agricultural University [J]. Jiangxi Science, 2024, 42 (04): 880-885.

[6] Y. Tian, W. Wang, J. Shang, et al. Research on the ideological and political construction plan of the computer composition principle course based on the OBE concept [J]. Shaanxi Education (Higher Education), 2024, (12): 33-35.

[7] N. Wang, J. Xu. Exploration on the reform of environmental microbiology heuristic classroom teaching [J]. China Educational Technology and Equipment, 2023, (24): 126-128.