Some Ideas on Construction of Course of Mathematical Foundations in Information Security

Yuechuan Wei
Electronics Technology Department
Engineering University of Armed Police Force
Xi'an, China
wych004@163.com

***Abstract*—*Information Security Mathematical Foundations* is one of necessary and backbone undergraduate courses of students major in network and information security. This paper analyses the current situation and difficultly encountered in this course. Combining with some practice of constructing high-quality *Information Security Mathematical Foundations*, this paper discusses the way of constructing a high-quality course from several aspects, such as teaching methodology, faculty qualification, teaching resource, and laboratory building and so on. "Combination between teaching and research", "MOOC education", "BOPPPS teaching mode" is introduced to improve students' activity and creativity.**

Keywords*—*Teaching method; MOOC education; High quality course

I. INTRODUCTION

Modern society has stepped into information times. Computer and network has brought tremendous convenience to our lives. At the same time, information leakage and malicious destruction threats information security greatly. Using modern information security technology, such as data encryption, digital signature, identity authentication and so on, can solve many information security problems. To satisfy the need of national information construction, information security education and talent cultivation become an important issue. Information security involves many subjects such as communication engineering, cryptography, computer science and technology, artificial intelligence and so on, among which mathematics provides a necessary base and plays an important role. Therefore, most of universities take *Information Security Mathematical Foundations* as a compulsory course of network and information security specialty.

For last decades, China has made a great achievement in information security construction. However, an undeniable truth is that our developments lag behind other advanced nations especially in core science and technology[1]. This is quite related to our basic education, research environment and so on, which implies that it is still a long-term arduous task in basic education transformation. How to form a scientific and practical education process for students to make them master knowledge firmly and keep innovative motivation is a focus in information security course construction. Therefore constructing high-quality course become especially important.

Combining with some practice of constructing high-quality *Information Security Mathematical Foundations*, this paper discusses the way of constructing a high-quality course from several aspects, such as teaching methodology, faculty qualification, teaching resource building, laboratory building and so on.

The remaining paper is organized as follows: Section 2 briefly introduces the course *Information Security Mathematical Foundations*. Section 3 presents some key problems in the process of education which restrict the quality of the course. In Section 4, we present some ideas and suggestions to construct high-quality course. Section 5 concludes the paper and summarizes our viewpoints.

II. BRIEF INTRODUCTIONS OF *INFORMATION SECURITY MATHEMATICAL FOUNDATIONS*

Information Security Mathematical Foundations is one of backbone courses of students major in network and information security. Its object is to teach the students to study and master the mathematical theory related to information security, mainly number theory, algebraic and computational complexity theory, especially to learn to use mathematical language strictly on information security and cryptography involved some specific mathematical theorems. Detailed reasoning and description of the algorithm is given and the key technology is involved. To make sure the students can keep up with the latest advances in information security and cryptography, and lay the foundation for the related research work and engineering practice[2-3].

Information Security Mathematical Foundations includes some obscure theory, such as group, ring, and field theory, elementary number theory, complexity theory relates to information security and so on[4-5]. Therefore, this course is a subject featured with theory and abstract content, involves a whole lot definitions and theorems, which makes it hard in the teaching and learning process. Traditional teaching methods which focus on theories understanding only, but ignore the practical applications of the contents in the area, will result in non-active, no goal when students learn the theory and

This paper is sponsored by the Natural Science Foundation of China for Young Scholars (No: 61202492).

technology, and reduce their interests in this course. Ultimately the teaching is infective. Because of that, studying how to construct the course, and improve teaching method to enhance students' learning motivation and promote their acquisition is an important subject for teachers.

III. Some Ideas on Construction of "Information Security Mathematical Foundations"

In this section, combing with our practical experience, we discusses the way of constructing an excellent course of *Information Security Mathematical Foundations* from several aspects, such as teaching methodology, faculty qualification, teaching resource building, laboratory building and so on.

（1） Building first classic teaching faculties

Considering as the first resource, teaching team is a decided factor for course construction. To build a teaching team which skills in information security technology, it is important to build an team with academic structure, age structure, professional title structure, academic structure, discipline more rational, and realize the combination of the high academic-level and high teaching-level.

To build an excellent course, effect of young teachers should be emphasized. Younger's can acquire new knowledge faster, but they are lack of experience and skills of passing on knowledge. So their teaching technique should be improved through training and guidance from experienced teachers. The corresponding strategies include collective preparation of instruction, perfection of teaching content, evaluation of teaching quality and so on, which guarantee young teachers grow rapidly.

（2） Improve teaching methods, employ multi-dimensional teaching mode.

To a large extent, learning quality depends on whether students are interested in what they learn or not, and whether their enthusiasm is aroused or not. In traditional teaching of *Information Security Mathematical Foundations*, teachers often focus on rigorous teaching structure and high-strength practice. For mathematics theories, teachers usually present the proof directly, while for problems, teachers usually present the complete resolution method directly. This will consequently make students passive, and there will be no space for students to thinking about how to solve problems by themselves. If the course goes on like this, students will lose their problem-solving ability by mathematics method. On the other hand, the course *Information Security Mathematical Foundations* is usually a specialized course for senior undergraduates, who put more attention on finding job or preparing postgraduate entrance examination. So if teaching is lack of interactive sessions and has no adequate interesting, it is difficult to arouse students' learning initiative.

To take full advantage of resource and introduce new teaching idea can help to attract students' interests. Web-based instruction, media technology, reference data, combination with complete and wonderful PPT lecture notes, will make teaching more vivid and impressive.

For expanding teaching resource, traditional classroom education with MOOC (Massive Open Online Courses) education can be combined together. For improving teaching methods, new teaching idea can be employed. For example, BOPPPS mode is a good choice, which means divide teaching into several stages, namely Bridge-in, Learning Objective, Pre-test, Participatory Learning, Post-assessment and Summary. BOPPPS mode is highly encouraged by many famous universities of North America [6-7]. By introducing BOPPPS teaching mode for reference, and using flexibility and intuitively means, teachers encourage students to take part in teaching activities, thus make them understand and master what they are learning. In table 1, we take course content of *Chinese residue Theorem* as an example of designing a BOPPPS teaching class, to explain how this effective teaching mode can be used to *Information Security Mathematical Foundations*.

TABLE I. *Class Design of Chinese Residue Theorem For Reference*

No	Name	Main Task
1	Bridge-in	Introduce question of "unknown number" in 《Master Sun's Arithmetical Manual》.
2	Learning Objective	State congruent equation and solve it with Chinese residue theorem.
3	Pre-test	Test basic concept of congruent equation, and methods to solve it.
4	Participatory Learning	Separate students into several group, let them try to solve the equation, then they present their difficulty encounter, and give the Chinese residue theorem.
5	Post-assessment	Give an example and let students solve the equation by using Chinese residue theorem.
6	Summary	Conclusion with question and answer.

（3） Combing teaching with scientific research, and highlighting course's characteristics

In construction of *Information Security Mathematical Foundations*, we should not only encourage teachers to devote themselves to participate in teaching, but also should encourage them join in scientific research and academic exchange at home and abroad. Combination of teaching and scientific research advances the innovation abilities and the colligation diathesis of students. The fast updating speed of information security especially needs combination of teaching and research, for the purpose that teachers could view knowledge hierarchy in academic frontier. And this would finally be embodied in course content. So, teachers should be encouraged to take part in developing research project according to their academic background and feature. At the same time, by taking the advantage of colleges' exchange, teachers should go out to serve as visiting scholars, to absorb excellent research methods and teaching achievements, which will finally support the construction of the course.

After students learn the basic knowledge of the course, they could also do science research on some specific point of some frontier problem. During their research, they could be guided to think deeper, their performance ability could be improved and their innovative thinking could be well trained.

As demonstration course, there must be some characteristic with the excellent course. Otherwise, the course is out of vitality. Characteristic could not only be found in content design and teaching system, but also could be reflected in teaching method. The excellent course should be well combined with the reality, the content should be exquisite and the model should be novel.

（4） Construct a reasonable knowledge system, and built the experiment teaching platform

The teaching content should be designed from top to bottom while the details should be introduced from bottom to top. The teaching content is introduced as a whole first and then in detail. The connection among the knowledge points should be paid attention to. The analysis and design should be done after the basic principles are clear. Due to the difference among the students' ability of taking and observing the knowledge, different students' need should be considered. In order to reach that purpose, teaching contents can be set into basic part and senior part in the course system. Students can choose appropriate teaching contents and corresponding experiments according to their base, ability and interest. Then the levels could be reflected in teaching. Besides, the build of a reasonable knowledge system need the focus on excellence. The related teaching material also need revised, completed and updated. No best, just better.

In order to improve the students' performance ability totally and strengthen the practice teaching, it would be a critical part to build some experiment platforms about basic cipher algorithm. There is strong relationship between the experiment platform and teaching effect. The cipher algorithm experiment platform or cryptanalysis experiment platform could offer students full training.

IV. SUMMARY AND CONCLUSION

Course constructing is a system project, which involves faculty qualification, teaching contents, teaching methodology, teaching means, teaching manage and so on. There are some thinking conclusions about *Information Security Mathematical Foundations* course constructing practice. First class teachers, multidimensional teaching mode, laboratory and combination between teaching and research play an important role in constructing *Information Security Mathematical Foundations* course. During the course constructing, the teaching idea of *all for students* should be insisted on and students' participation should be encouraged. The main purpose is to increase students' ability and innovative thinking which can reflect the teaching effect.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their valuable remarks. This work is supported by the Natural Science Foundation of China for Young Scholars (No: 61202492).

REFERENCES

[1] Wei Y, Rong Y. Some Ideas on Construction of Course of Cryptography in Computer[J]. Journal of Northwest University (Natural Science Edition), 2014()44:125-127.

[2] Gongliang Chen. Information Security Mathematical Foundations[M]. Tsinghua University Press. Beijing. 2006:4-150.

[3] Zhongping Qin, Huanguo Zhang. Information Security Mathematical Foundations[M]. Tsinghua University Press. Beijing. 2006:50-83.

[4] Zhu Q, Li X, Xu J, Ma Y. Research on New Teaching Methods of Information Security Mathematical Foundations[J]. Computer Education, 2014(1):43-47.

[5] Fu S, Liu D, Zhao W, Ren J. Applitions of BOPPPS Mode in Class of Information Security Mathematical Foundations[J]. Computer Education, 2015(6):22-25.

[6] Pattison P, Russel D. Instructional Skills Workshop(ISW) Handbook[M]. Vancouver: UBC Center for Teaching and Academic Growth, 2006:42-63.

[7] Allan J. Learning Outcomes in Higer Education[J]. Studies in Higher Education, 1996, 21(1):93-108.