Some Thoughts on the Teaching of Fundamentals of Mathematics in Information Security

Teng Guo*

School of Cyberspace Security, University of International Relations, Beijing 100091, China

guoteng@uir.edu.cn

Abstract. The course of fundamentals of mathematics in information security aims to provide necessary knowledge and technical tools for pursuing future careers in information security. In this paper, we try to present some thoughts on the teaching of this course. The contents of this course include: number theory, algebraic theory, information theory, complexity theory, combinatorics, mathematical logic et al. Due to the limit of study hours, the teachers have to choose the most basic and relevant topics. Based on our nine-years teaching experience on this course and related courses, we organize the selected topics of this course into 30 study hours. Furthermore, the selected topics are supported by immediate usages in concrete cryptography schemes. At last, the interdependence of the selected topics is discussed, so as to provide useful references to peers and self-study students.

Keywords: Fundamentals of mathematics, Information security, Cryptography

1 Introduction

The teaching of fundamentals of mathematics in information security plays an important part of cultivating information security professionals. Learning in this area requires students not only to have a solid foundation in mathematics, but also to be able to apply the knowledge to solve real-world information security problems. Students can easily get frustrated during the study process, especially when encountering some difficult topics. There are many studies to motivate the interests of students. [1, 2] exploited the relationship between fundamentals of mathematics and cryptography. [3] proposed to use an interactive approach during the course to draw the attention of students. [4, 5] studied the inter-correlation between topics of fundamentals of mathematics. [6] studied the job-market of information security and summarized the most needed techniques. [7, 8] explored the interdisciplinary between many courses and proposed a hybrid mode for teaching. [9] summarized the prerequisite knowledge of information security to perform job responsibilities.

In the process of teaching, there are some issues that deserve in-depth consideration. First, traditional textbooks often focus on the explanation of basic concepts and techniques, but lack innovation and practicability. In order to enhance students' appli-

Y. Feng et al. (eds.), *Proceedings of the 2024 3rd International Conference on Educational Science and Social Culture (ESSC 2024)*, Advances in Social Science, Education and Humanities Research 914,
https://doi.org/10.2991/978-2-38476-384-9_11

cation ability and study interests, the teaching mode that combines practice and theory should be strengthened. Furthermore, classic cases in the field of information security should be introduced to allow students to apply their acquired knowledge and skill to analyze practical cases. At the same time, the basic course of fundamentals of mathematics in information security should be combined with practical application scenarios, focusing on practical training in teaching, and guiding students to actively participate in project development, such as message encryption and decryption, so as to improve their information security thinking. Second, in terms of teaching methods, teachers need to abandon the restraint of traditional teaching models and explore more flexible teaching methods. For example, the teacher can increase interactivity in teaching, and divide students into small groups for discussion and evaluation. Multimedia technologies, such as digital projector and animation, are used to assist teaching and make the course content more concrete, intuitive, and easy to understand. In addition, teachers can also make use of online resources, such as MOOCs and online courses on Bilibili., to provide students with diversified learning resources to meet their different needs and interests. Finally, in terms of teaching evaluation methods, most of the existing evaluation methods are biased towards the traditional paper written test, which cannot fully and objectively reflect the ability and performance of students. In order to evaluate students' abilities more accurately, a multi-perspective evaluation system should be established. For example, hierarchical and staged assessments can be adopted, and students can be required to submit assignments, participate in class discussions, etc. At the same time, teachers should also innovate on the basis of existing teaching materials, compile a set of practical assessment systems, and evaluate students in stages, so as to better stimulate students' interest in learning and improve the quality of education.

In one word, the basic teaching of fundamentals of mathematics in information security needs to be continuously innovated and improved. The teaching mode combining practice and theory should be strengthened, more flexible teaching methods should be explored, in order to lay a solid foundation for the students’ future information security professionals.

2 Thought on the content of the teaching

The fundamentals of mathematics in information security includes many branches of mathematics and computer sciences, such as number theory, algebraic theory, information theory, complexity theory, logic theory and combinatorics. The basic objective of this course is that students should master the most basic and relevant topics and get a solid foundation for subsequent studies. In the following, we try to give a detailed explanation on the scope of fundamentals of mathematics in information security.

1. Fundamentals of number theory: (1) integer and divisibility, which involve the concept of divisibility, Euclidean algorithm, greatest common divider and least common multiple, etc. (2) congruence and modulo operations, which include the properties of congruence, residual systems, Euler's function and Euler's theorem, Sun Tzu's theorem, etc. (3) primitive roots and orders, which include the concept of

primitive roots, how orders are calculated, and how to find primitive roots. (4) prime test, which includes simple deciding method, deterministic deciding method and probabilistic deciding method.

2. Algebraic theory: (1) group theory, which involves: the concept of groups, subgroups, homomorphism and isomorphism, regular subgroups and quotient groups, cyclic groups, permutation groups, and their applications in cryptography. (2) rings and fields, which include the concept of rings, sub-rings, whole rings, dividing rings, and fields, ideals, expansion of fields, finite fields, and their applications in cryptography, such as NTRU ciphers. (3) polynomials, which include unary polynomial rings, polynomial division, factorization, roots of polynomials, and polynomials over finite fields.
3. Elliptic curves: (1) preliminary knowledge of elliptic curves, which involves the basic concepts and properties of elliptic curves. (2) operations on elliptic curves, which includes addition, multiplication, and other operations on elliptic curves. (3) discrete logarithm problem on elliptic curves, which is the basis of elliptic curve cryptography.
4. Shift register sequence: (1) basic concepts of shift registers and shift register sequences, which involves the concepts of linear shift registers and nonlinear shift registers. (2) linear shift register sequence, which includes the space of the sequence, periodicity and m-sequence of the linear shift register. (3) nonlinear shift register sequences, which includes a brief introduction to the concept of nonlinear shift register sequences and correlation immune functions.
5. Information theory and complexity theory, which include fundamentals of information theory, entropy, mutual information, the mathematical model of the security system, and the time and space complexity of algorithms, reductions, NP complete problems.
6. Combinatorics, which includes permutations and combinations, principle of inclusion and exclusion, generating functions, Polya counting principle, block design.
7. Mathematical logic, which includes classical propositional logic, classical first-order logic, modal logic, BAN logic, Kailar logic, and timing logic and their applications in information security.

In one word, the fundamentals of mathematics in information security cover multiple branches of mathematics such as number theory, algebra, elliptic curves, shift register sequences, information theory and complexity theory, combinatorics and mathematical logic. Information security needs a solid and extensive mathematical foundation for future researches. Due to the limit on the total number of study hours (each includes 45 minutes) on this subject, the teacher has to select the most basic and relevant topics for this course. For example, in University of International Relations, this course is assigned 30 study hours in total. After extensive investigation and exhaustive discussion, the following topics are selected in the teaching of this course, which are organized in Table 1.

Table 1. Content arrangement in the teaching of fundamentals of mathematics in information security.

Serial number	Contents	Number of study hours
1	Divisibility theory	4
2	Congruence theory	6
3	Number theory functions	6
4	Quadratic remainder theory	4
5	Primitive element	4
6	Finite fields	6

3 Thought on the method of the teaching

With the development of modern technology and online courses, students are eager to learn the most useful knowledge, and especially hope to have a deep understanding of the underlying principles. Fortunately, there is a close and important relationship between the fundamentals of mathematics in information security and cryptography, which usually can stimulate students' interests. We elaborate the above relationship from the following aspects:

1. The fundamentals of mathematics in information security constitute the cornerstone of cryptography. As a core discipline in the field of information security, the research and practice of cryptography are inseparable from the profound mathematical foundation. The mathematical foundation provides necessary theoretical support for the algorithm design, algorithm analysis and implementation of cryptography. For example, the concepts of factorization and congruence in number theory play an important role in public-key cryptography. The structures of groups, rings, and fields in algebraic theory provide a theoretical basis for symmetric cryptography.
2. Cryptography is an application field of the fundamentals of mathematics in information security. The research content of cryptography mainly includes cryptographic algorithms, cryptographic protocols and cryptosystems. The design and analysis of these schemes need to rely on the knowledge of the fundamentals of mathematics in information security. For example, in the design of cryptographic algorithms, it is necessary to use the counting principles and calculation methods to ensure the security and efficiency of the algorithm. In the design of cryptographic protocols, it is necessary to verify the correctness and security of the protocol with the help of logical reasoning or reduction methods.
3. The fundamentals of mathematics and cryptography jointly ensure information security. The combination of fundamentals of mathematics and cryptography provides a strong guarantee for information security. Through cryptography algorithms, digital signatures and cryptography protocols, the confidentiality, integrity

and authenticity of information can be ensured. The fundamentals of mathematics provide a solid theoretical foundation and algorithm support for information security. The two complement each other and constitute the core components to protect information security.

4. Case studies. Taking public key cryptography as an example, it makes use of the large integer factorization problem in number theory to ensure the security of the private key. Generally, the cryptographic algorithm in public key cryptography is often based on some hard mathematical problems, such as large integer factorization and discrete logarithm, which make it nearly impossible to decipher ciphertext without a key. This question is also one of the research contents in the field of number theory of the fundamentals of mathematics. Therefore, to a large extent, the security of public key cryptography depends on the support of fundamentals of mathematics in information security.

From the above analysis, we can see that there is an inseparable relationship between the fundamentals of mathematics in information security and cryptography. They are interdependent and mutually reinforcing, and together they provide a solid theoretical foundation and technical support for the development of information security. Figure 1 describes the relation diagram between the fundamentals of mathematics and cryptography.

For example, after introducing Sun Tzu's theorem which can map some large congruence class into several smaller congruence classes. We immediately presented the concept of secret sharing in cryptography, which requires some dealer to distribute a secret value to several participants. Clearly, the above two processes share many similarities. However, we point out that the directive usage of Sun Tzu's theorem to implement secret sharing has the security defect that it will leak some information about the secret. Hence some modifications have to be made when using Sun Tzu's theorem to implement secret sharing. Equipped with the useful knowledge that are just learned and guided by concrete problems, the passion for learning is inspired that many students are not satisfied with just solving textbook problems.

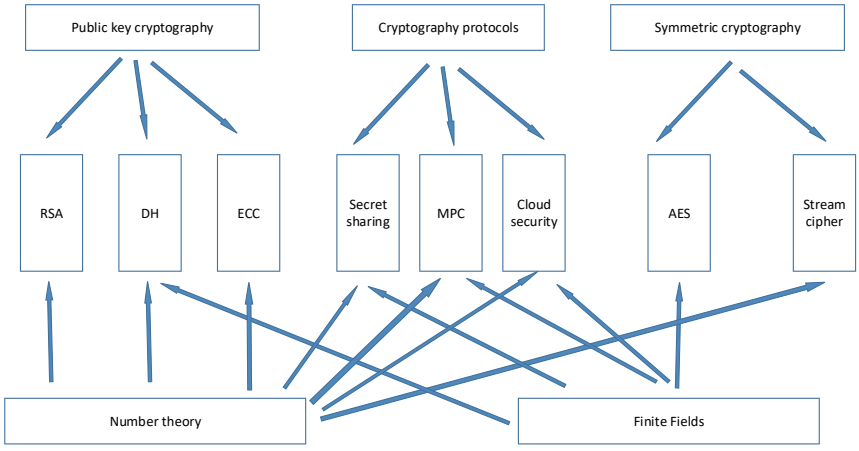

Fig. 1. The relationship diagram between the fundamentals of mathematics and cryptography.

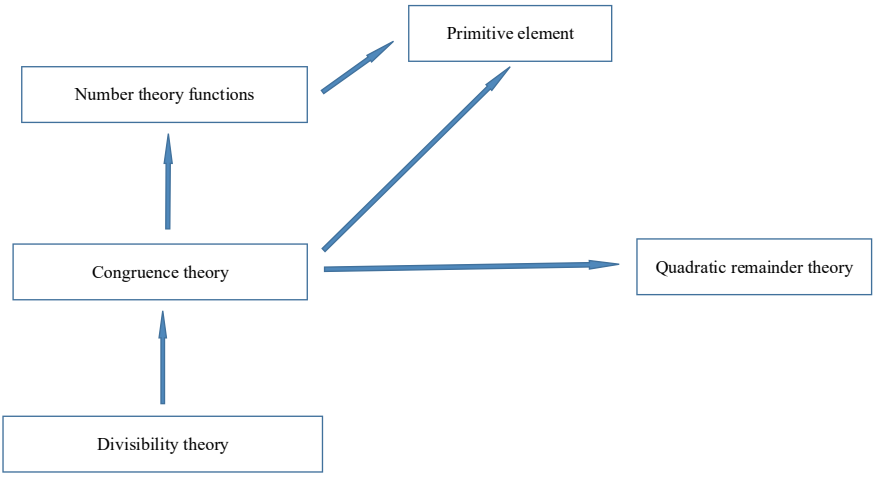

Fig. 2. Knowledge structure of fundamentals of mathematics in information security.

Furthermore, the topics in fundamentals of mathematics in information security are interdependent. From divisibility theory, Gauss invented congruence theory, which is the foundation for number theory functions, quadratic remainder theory, primitive element and the computation of order. Besides, the Euler totient function is an easy-to-use tool to analyze primitive element. Figure 2 describes the knowledge structure of fundamentals of mathematics in information security. By showing the interdependence of the topics of fundamentals of mathematics, students can have constant interests during the study of this course. In our university, the question and answer time can lasts for two to four hours each week, and some students can even bring up multiple solutions to some challenging problem. Based on teaching practices and students feedback, the course achieves the aim that students not only master the basic knowledge of mathematics required in information security, but also can apply this knowledge to practical problems, improving their application ability and innovation ability. Besides, as an important basic course in information security, it is of great significance for promoting the development of the discipline. From this course, students can learn about the latest advances and cutting-edge technologies in information security, contributing to the development of the discipline. In the future, more case studies will be added to further improve students' problem-solving ability. At the same time, more modern mathematical theories like algebraic number theory and algebraic geometry and more cryptography ideas like obfuscation and fully homomorphic encryption can also be introduced to enrich the content of this course.

4 Conclusion

With the development of network technology and online courses, students have multiple ways to access knowledge. However, the subject of mathematics is generally not friendly for self-study, even with the help of online courses. To stimulate the learning

interest of students and provide a reference for peers, we first review the content of the fundamentals of mathematics in information security, and then elaborated the usefulness of the topics in concrete applications. By exploiting the relationship between this course and cryptography and displaying the immediate use of some just learned knowledge and tools, the students can have constant interests during the study of this course. By communicating some useful experiences, we hope that the learning outcome of this course may get better and better, and students can obtain a firm theoretical foundation for future careers in information security.

Acknowledgments

This work was supported by Research Funds for NSD Construction, University of International Relations, grant No. 2024GA06.

References

1. Dengguo Feng. 2002. Research status and trend of cryptography at home and abroad, Journal on Communications. vol 23(5), pp. 18-26
2. Zhijun Li, Minghong Liao. 2006. Research on Cryptography Teaching, Computer Education, vol. 9, pp. 18-26
3. Weidong Qiu, Kefei Chen. 2007. New Interactive Model in Information Security Mathematics Teaching, Computer Education, vol.10, pp.19-21
4. Xinglan Zhang. 2011. Teaching Research of Mathematic Course in Information Security, Computer Education, vol.13, pp.45-46
5. Jie Zhou, Jing Han. 2020. Exploration of the Teaching Mode of Mathematics Foundation of Information Security Based on the Difficult Problems of Cryptography, Modern Computer, vol.2, pp.57-61
6. Qiang Liu, Peidai Xie, Xingkong Ma, Wentao Zhao, Shaojing Fu, Yongjun Wang. 2024. Exploration of comprehensive reform of cyber security curriculum driven by job competency demand, Computer Education, vol.6, pp.178-182
7. Shufen Niu, Fei yu, Pingping Yang, Lizhi Fang. 2021. Research on the basic theory and practical teaching methods of information security mathematics in the context of interdisciplinarity, Computer Education, vol.2, pp.149-152
8. Yihua Zhou, Weimin Shi, Yuguang Yang, Bo Zhang. 2020. Exploration on the Construction of Hybrid Course of Cryptography, Innovation and Practice of Teaching Methods, vol.3(16), pp.5-7
9. Michael E. Whitman, Herbert J. Mattord. 2017. Principles of Information Security, Cengage Learning, 6th edition.