Advances in Social Science, Education and Humanities Research (ASSEHR), volume 184
2nd International Conference on Education Science and Economic Management (ICESEM 2018)

Teaching and Practice of *Information Security Conspectus* Based on Case Teaching

LIU Xin
School of Information Engineering
Shandong Youth University of Political Science
Jinan, China

***Abstract*—*Information Security Conspectus* is a comprehensive course of information security technology. In view of the following reasons, it is often difficult for teachers to achieve the ideal teaching effect, i.e., existing teaching textbooks cannot provide a rich "entry level" case, and the teaching content of the course is difficult to closely connect with a large number of preamble courses. Therefore, this paper put forward the following teaching reform ideas, i.e., reconstructing teaching contents, introducing case teaching and reforming examination methods. In view of the penetration of cryptography to the teaching contents of each module of the course, a detailed teaching case design of "bitcoin and block chain" was put forward for the teaching module of cryptography. In addition, specific ideas for setting up teaching cases was also provided, which shows that cryptographic technology can also be applied in other teaching modules of the course.**

Keywords*—*Higher education; Curriculum reform research; case teaching; Innovation ability

I. INTRODUCTION

Information Security Conspectus is a basic course for information security specialty, and also an important elective course for computer related majors. In our school, it has been classified as a professional elective course in the computer science and technology major. The teaching goal of this course is to make the students not only master the basic knowledge of information security, but also enhance the awareness of information security and improve the ability to ensure information security in daily life, work and study to lay the foundation for further study of the follow-up information security class. Although it is only an elective course, it is very difficult to teach. The reason lies in the fact that compared with other specialized courses, the course has the following characteristics: strong comprehensiveness, fast updating of teaching content, closely related to many professional courses, and strong practicality [1].

II. THE TEACHING CONTENT OF THE COURSE AND THE GOAL OF TEACHING REFORM

In the process of teaching, we find that there exist the following problems: 1) Teaching content is extensive, and context setting is not consistent in different textbooks. 2) It is difficult to find an entry level textbook that is easy to read and can provide rich examples. 3) Because some teaching contents are difficult and abstract, students' enthusiasm in class is not high. In order to improve the teaching effect, we have tried teaching reform in the following aspects: 1) Carefully select the content of the course. At present, the theoretical part of the course is 32 hours. In addition to the tests conducted in the classroom, we divide the remaining teaching content into six modules, such as course guidance, cryptography, network security, information system security, information content security and cloud computing security (as shown in Figure 1).

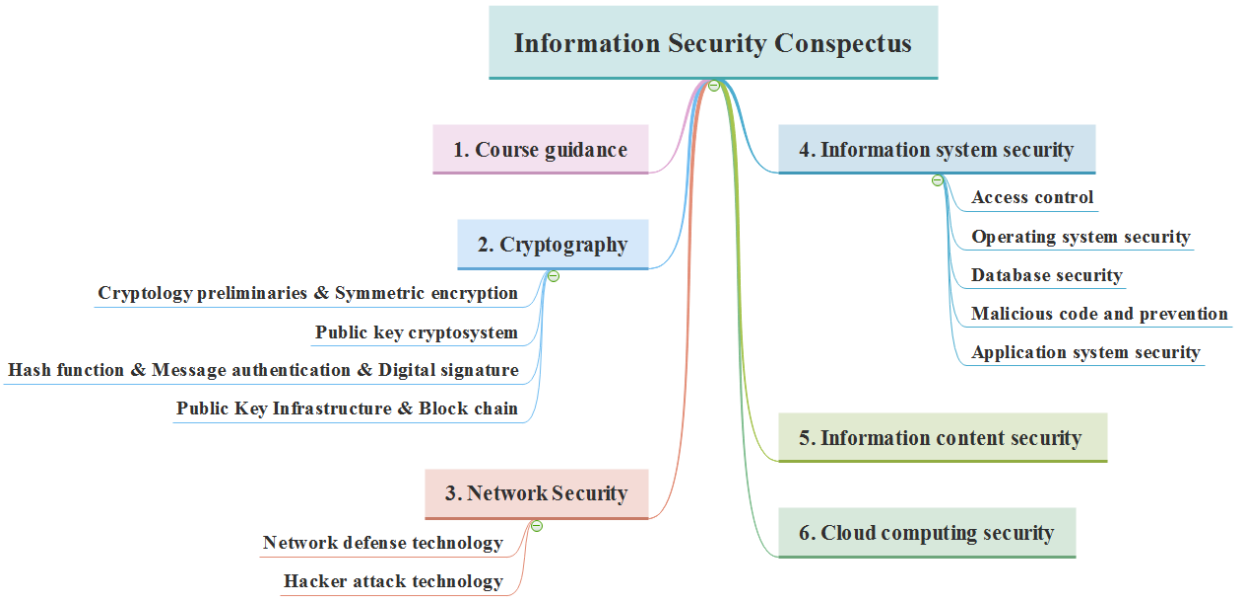

Fig. 1 The module division of the course content

2) Adopt case teaching method. Enrich teaching content by introducing practical application cases. 3) Introduce a variety of assessment methods to stimulate students' interest in learning and improve their understanding of the importance of information security and the degree of knowledge of information security in various fields.

III. CASE TEACHING DESIGN BASED ON CRYPTOGRAPHY

A. *Case teaching method*

The feature of the case teaching method is to teach by using the problems in reality. In the course of teaching, the teachers lead the students to analyze the problem together, discuss the solutions, and introduce the knowledge points in the process of solving the problem [2]. At present, case teaching has been widely applied in various courses teaching. We also try to introduce this method in daily teaching for the following three advantages: 1) It helps to make up for the lack of textbooks and stimulate students' interest in learning. 2) Being guided students to discuss problems in teaching case, students can deepen their understanding of what they have learned. 3) We can use case teaching to link up the knowledge points in each teaching module and build a complete knowledge system.

B. *The concrete implementation of case teaching method*

1) Case introduction

In this section, we selected "bitcoin and block chain" as the teaching content, and designed a case discussion lesson based on the anonymous transaction protocol based on bitcoin in [3]. Before this class, students have learned classical cryptography such as symmetric ciphers, public key ciphers, hash functions, digital signatures and so on, but they also need a comprehensive teaching case that can reflect the latest applications of cryptography (especially the secure electronic trading protocol). By introducing this case, we can help students understand the basic principles of bit coin trading. Using the methods in [4], we divided the teaching objectives of this class into the following three levels: knowledge goals, skill goals and emotion goals. 1) The knowledge goals include understanding P2P (Peer to Peer) network, block chain, bitcoin, bitcoin address, mining and transaction anonymity and so on, and understanding the specific composition of the block. 2) The skill goals include mastering common symbols in the description of cryptographic protocols and understanding block addition technology, the specific process of bitcoin trading, and workload proof technology. 3) The emotion goals include stimulating students' interest in cryptology knowledge through the latest application of cryptography to lay the foundation for the design of cryptographic protocols in the future and to cultivate their ability to think deeply and innovate.

2) Case launches

In the course of teaching, we first introduced the concepts of P2P network, bitcoin address, bitcoin, block chain and the process of encryption and decryption. Then, we explained the process of bitcoin transaction carried out by customer Alice and store B (as shown in Figure 2). Finally, we helped students to understand the design method of the security electronic transaction protocol through the discussion.

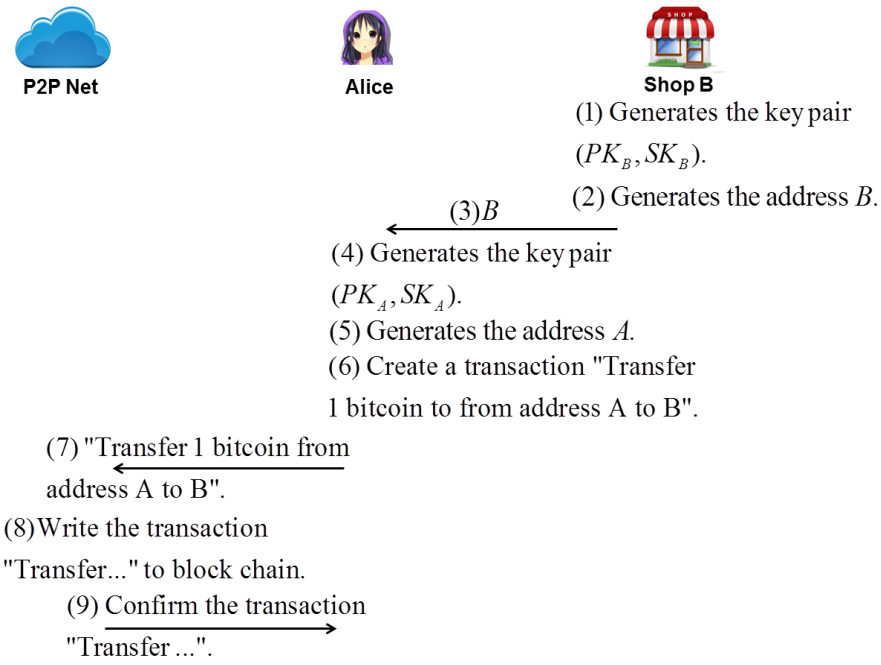

Fig. 2 The teaching case of trading in bitcoin

In the course of the discussion, the following questions should be raised to students:

Question 1: What is the relationship between bitcoin and P2P network?

Explanation: The bitcoin transaction is implemented based on the P2P (Peer to Peer) network composed of all bitcoin users of the world, which can be seen as a payment and settlement system based on the P2P network.

Question 2: What is the relationship between block chain and bitcoin?

Explanation: Bitcoin is a kind of "virtual currency" used for trading, and every transaction record needs to be saved in the "account book" based on block chain.

Question 3: How to determine whether Alice has successfully paid bitcoins to B?

Explanation: Alice's request for transfer to B is confirmed by the P2P network, that is, the corresponding transaction record has been added to the block chain.

Question 4: Why do we need to a build block head in each block?

Explanation: There are two hash values in each block, which makes it impossible for an attacker to tamper with the transaction records in the block.

Question 5: How to prevent miners from forgery of bitcoin?

Explanation: Ask the miner to provide a proof of workload.

Question 6: Can the above transaction process protect Alice's privacy?

Explanation: The answer is affirmative. The transaction between Alice and B is confidential to the outside world (i.e., the entire P2P network), because the outside world only knows that bitcoin is transferred from the address A to the address B, but is unable to know the specific identity of the parties.

3) Case summary

In this lesson, we gradually expanded the content of the teaching cases, so that students finally understood the whole case. At the same time, through question discussion, we led them to deepen their understanding of teaching content (bitcoin transaction protocol). In addition, students had a deeper understanding of the practical application of digital signature and hash function, and further realized that adding new block to block chain (i.e., mining) demands a large amount of computation.

4) Other representative cases

In the course of *Information Security Conspectus*, we use 8 hours to teach cryptography modules, and end with the comprehensive case of block chain. In fact, cryptographic technology has also penetrated into the following teaching contents. 1) In teaching access control technology, we think that in addition to introducing typical access control models (autonomous access control, strong access control and role-based access control), it is necessary to introduce access control mechanisms to confidential files. Therefore, we need to use cryptography. 2) In the part of operating system security architecture, the authentication mechanism constitutes the outermost layer of the whole security system, and this kind of technology is realized by authentication protocols in cryptography. 3) In the field of database security, in order to encrypt data, it is necessary to construct a key protection chain composed of server master key, database master key, digital certificate, asymmetric key and symmetric key, which is exactly corresponding to key management technology in

cryptography [5]. 4) In the field of information content security, cryptography is an important foundation for digital watermarking and digital copyright protection. 5) In the field of cloud computing, the major security threats to various cloud services include traffic eavesdropping, malicious media, denial of service, lack of authorization, weak authentication, virtualization attacks, and overlapping of trust boundaries [6]. At the same time, in order to solve these problems, we need to comprehensively use cryptography technology such as encryption, hash function, digital signature, public key infrastructure, identity authentication and so on. In order to help students understand the specific application of cryptography in the above fields, it is necessary to design cases carefully and introduce them into the classroom. In [7], an interesting story was introduced by Bethencourt et al. The FBI anti-corruption branch in Knoxville and San Francisco was jointly investigating a case, which demands to implement access control to investigation files. At the same time, the following three categories of people were allowed to view the secret files: 1) FBI agents in Knoxville or San Francisco, 2) Executives with more than 5 management levels in FBI, 3) A special consultant named Charlie Eppes. In order to achieve the above access control targets, “FBI agent”, “Knoxville”, “San Francisco”, “Management level above 5” and “Charlie Eppes” were regarded as user attributes. Therefore, the access control rules could be represented as follows.

$$((\text{"}Public\ Corruption\ Office\text{"})\ AND\ (\text{"}Knoxville\text{"}\ OR\ \text{"}San\ Francisco\text{"}))\ OR\ (\text{"}Management\text{-}Level > 5\text{"})OR\ (\text{"}Name : Chalie\ Eppse\text{"}).$$

Then, the content of files was protected by attribute encryption technology. According to this story, we designed a teaching case. Concretely, in the access tree as shown in Figure 3, the process of accessing the content of a file can be viewed as a process of backtracking from one or more leaf nodes to the root node. In this process, users needed to use the attributes they have to open the “AND” gate or “OR” gate for implementing access control. When they opened the “OR” gate at the root node, they can access the file content.

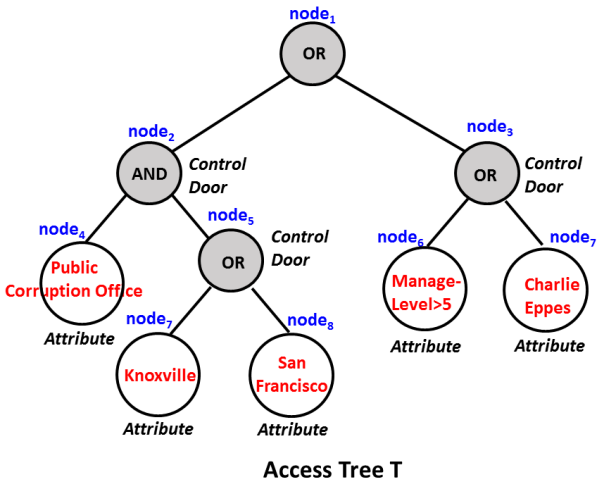

Fig. 3 The teaching case of access control of secret files using attribute encryption

IV. CONCLUSION

In this paper, we apply the case teaching method to introduce the application of modern cryptography to the course of *Information Security Conspectus*, and provide a detailed design of a comprehensive teaching case (i.e., the bitcoin transaction protocol). We emphasize that cryptography is the core of modern information security technology, and cryptography is also widely permeated in all the teaching modules of *Information Security Conspectus*, so it is especially suitable for the adoption of case teaching. In the future, we will further design teaching cases that can reflect the latest practical applications, and develop curriculum experiments for these cases.

ACKNOWLEDGMENT

This research was financially supported by the project of Shandong province higher educational science and technology program (Grant NO. J17KA081) and the teaching reform research project (of the year 2018) of Shandong Youth University of Political Science--The problem-driven teaching reform and practice of data structure and algorithm series course.

REFERENCES

[1] Z. Li, S. Li, and J. Liao, “Study and practice on the course teaching of information security introduction,”Computer Education. Beijing, pp. 15-18, February 2011. (In Chinese)

[2] Y. Cui, S. Ren, J. Liu, and J. Liu, “Case-driven teaching reform on computer programming for non-computer majored college students,”Journal of North China Institute of Aerospace Engineering. Langfang, vol. 28, 50-52, January 2018. (In Chinese)

[3] Y. Hiroshi (Book), Z. Zhou(Translated), Graphic Cryptography, 3rd ed.. Beijing: People’s Post and Telecommunications Press, 2016, pp. 365-372. (In Chinese)

[4] Y. Yang,“C language teaching design based on case teaching method,” Computer Era. Hangzhou, pp. 104-106, June 2016. (In Chinese)

[5] P. Chen, T. Zhang, and M. Zhao. Information system security. Beijing: Tsinghua University Press, 2016, pp. 210-212. (In Chinese)

[6] T. Erl, R. Puttini, and Z. Mahmood. Cloud computing: concepts, technology & architecture. Pearson Education, 2013, pp. 126-129.

[7] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. Proceedings of Security and Privacy 2007 (S&P 07), New York: IEEE Press, 2007, pp.321-334.