Yi SUN[1], Jianmin DONG[1], Hongwei GUO[1], Liang WANG[1], Zhaohai RAN[2]

College of Information Engineering, Tibet Institute for Nationalities (1), Network Information Center, Tibet Institute for Nationalities(2)

Teaching Research on Cryptography in Computer Science and Technology Specialty

Abstract. *With the speeding up of global information pace, the security of network information is becoming an increasingly serious problem. As the related course of information security, cryptography turns into a basic and important course of Computer Science and Technology Specialty in universities. Based on an intensive study of this course, this paper probes into the effective teaching method of cryptography as well as the selection of textbook. The paper begins from designing theoretic and experiment teaching model, and then puts these models into practice. Thirdly, the paper provides corresponding assessment means to these models. Lastly, the paper puts the models into practical teaching and they are turned out to be effective and be of reference value.*

Streszczenie. *W artykule omówiono metody uczenia kryptografii. Przedstawiono teoretyczne i eksperymentalne doświadczenia oraz zaproponowano praktyczne przykłady nauczania kryptografii. (**Nauczanie kryptografii na specjalnościach technika komputerowa i technologia**).*

Keywords: cryptography; teaching design; computer science and technology
Słowa kluczowe: kryptografia, techniki komputerowe.

Introduction

In the last decade, the rapid development of network and information technologies caused multiple holes in network information security, and network information security has become the key issue in today's information technology world [1]. At present, an increasing number of universities in China have opened cryptography for the majors of computer science and technology, and it is the basic course for them, such as Peking University, Xidian University, Wuhan University, all of them have opened cryptography and cultivated a number of information security talents for our country [2]. Tibet Institute for Nationalities (TIFN) opened cryptography for the majors of computer science and technology in 2004, and established it as the core course for them.

Cryptography is a core curriculum for the majors of computer science and technology; it offers a powerful theoretical basis and practical application [3]. At the same time, it consists of a variety of subjects, such as Number theory, Programming algorithm, Encryption and Decryption practice [4]. It requires that students should not only have a certain ability of mathematics theory but they should also have that of programming, so it is possible to established cryptography as a compulsory course for juniors who major in computer science and technology.

Based on the teaching plan of this course, this paper brings forth the teaching method of combining theory and experiments with students' adaptive learning. In this way, students' interest can be evoked and their initiatives can be practiced. In the end, this paper sums up the teaching method and puts forward some thinking.

The exploration of teaching method

Cryptography is an interdisciplinary course that is composed of Mathematics, Computer Science and Communications and Information Systems. Since cryptography includes a large quantity of subjects, such as stream cipher, Data Encryption Standard (DES) algorithm, Advanced Encryption Standard (AES) algorithm, Rivest-Shamir-Adleman (RSA) algorithm, Key Distribution and Key Management, Message Authentication and Hash Algorithm, Digital Signature Algorithm (DSA), Password Authentication Protocol (PAP), etc. [5, 6] (The contained knowledge of cryptography is as table 1). Under this circumstances, how to ensure that students have an entire view of cryptography when they face so many contents? How can they master the basic models and theory? How can they do research initiatively? How can their research train of thought be cultivated? These questions are essential for cryptography teaching.

Table 1. Contained knowledge of cryptography

Sequence number	Contained knowledge of cryptography	
	Classification	Detailed contents
1	Basic concepts	Concepts of encryption and decryption, classification of cryptosystem, the concepts、feature and performance of symmetric key cryptosystem and asymmetric key cryptosystem
2	Typical algorithms	DES、RSA
3	Related technologies	PKI, key management protocol, digital signature

The periods of cryptography are limited, which requires students have a certain ability of mathematics theory（including their knowledge of Computational Complexity, Abstract Algebra, Arithmetic, Probability Theory, Combinatorics, etc.）to ensure that they can master the theory system in such limited periods. The main task of teachers is to explain the comprehension and application of algorithms in class and demonstrate the specific examples of algorithms in multimedia teaching. They need not explain the correlative mathematics theory, thus students' immersing themselves in bald mathematics which results in their losing interest in their learning can be avoided. During the course of teaching, letting the students make practice can enhance their understanding of algorithms, implement application of encryption and decryption, which can cultivates students' operability, and enhance their initiatives. Meanwhile, introducing the related and up to data research can widen the thought and view of students. And for the students of different levels, assign the exercise corresponding to their levels; in this way can students lead to adaptive learning. Thus it is not only helpful for students to master the theory of cryptography, spur them to explore the kernel of cryptography, but also beneficial to evoke their study interest, cultivate their ability of research and initiatives.

According to the above principles, there are 51 class hours teaching of cryptography curricula，34 periods for theory teaching, 17 periods for practical teaching. Some

courses must be opened before cryptography teaching, such as mathematics, data structures, advanced programming language, so that students can have a basis of cryptography theory.

During the course of theoretical teaching, in order to ensure that the students can understand and master the concepts of cryptography in the class, as well as establish the pattern of information security, the teachers apply multimedia teaching. So the course content is arranged as table 2.

(1) An introduction to cryptography (1 period): The teachers arouse the students' study interest through telling the application of cryptography in military in early stage, and form their initial impress of integer frame of cryptography, which can lay the foundation for their further learning.

(2) Classical cryptography (1 period): This course mainly asks students to give examples, in this way can students have a comprehension of substitution cipher and permutation cipher, lay foundations for the modern cryptography's study.

(3) Modern cryptography (2 periods): The students are asked to find relative information after class, explain the threats of information security, and establish the pattern of information security. The teachers must know the students' theoretical basis very well, and ensure that the students get some idea of modern cryptography.

(4) Stream cipher (2 periods): Through demonstrating the multimedia courseware, students can apprehend linear feed back shift register and master how to build nonlinear sequence.

(5) Block cipher system (8 periods): Detailed mathematics theory is not necessary for this course, what essential are students' practice of programming algorithms that they learned in the class with their knowledge of data structures and programming to master the DES algorithm, as well as enhancing their learning ability.

(6) Public key cryptography (8 periods): Just like block cipher system, mathematics theory is not necessary for this course, too. The core of this course is to demonstrate programming algorithms in class and help the students comprehend and master the RSA algorithm.

(7) Key distribution and key management (4 periods): Through teachers' citing examples and explaining the practical application, the students are asked to master key distribution and key management as well as achieve safety communications.

(8) Message authentication and hash algorithm (3 periods): Combining different application circumstance, the students are required to apprehend the function and principle of message authentication, in this way their practical interest is stimulated and whether the message they received is correct can be ensured.

(9) DSA and PAP (3 periods): The basic principle of DSA is explained and common basic algorithms are presented in class, and relative example is demonstrated to deepen the students' comprehension.

(10) Network encryption and certification (2 periods): Encryption and decryption are explained to students through examples, so that the students have a good knowledge of the process of encryption and decryption, and the certification patterns.

Table 2. Teaching design

Sequence number	Teaching design		
	Teaching contents	Periods	Teaching design
1	An introduction to cryptography	1	Arouse the students learning interest when they begin to learn cryptography, and form their initial impress of integer frame of cryptography
2	Classical cryptography	1	The students are required to cite examples
3	Modern cryptography	2	The students are required to seek information after class, expand the threats of information security, and establish the pattern of information security
4	Stream cipher	2	The students are required to apprehend linear feed back shift register and master how to build nonlinear sequence through demonstrating the multimedia courseware
5	Block cipher system	8	The students are required to implement the programming algorithms after class and master the DES algorithm through combining the knowledge of data structures and programming
6	Public key cryptography	8	The teachers are required to demonstrate programming algorithm in class, and in this way, help students master RSA algorithm
7	Key distribution and key management	4	The students are required to master the pattern of key distribution and key management
8	Message authentication and hash algorithm	3	The teachers demonstrate the teaching examples for students and require them keep abreast of related current information
9	DSA and PAP	3	The teachers are required to introduce the basic principle and common basic algorithms to students, the students are required to practice in practical process

Sequence number	Teaching design		
	Teaching contents	Periods	Teaching design
10	Network encryption and certification	2	The teachers are required to introduce the implement function of encryption and decryption algorithms, interpret the basic principle and application of encryption and decryption algorithms to students

Practical teaching

Cryptography is the basic and core content of information security, since it is of strong partiality, and it's a subject integrated with practice tightly. The ultimate aim of cryptography is afford various secure utility algorithms, it insist that theory is contacted with practice, so its practical teaching must be strengthened. The students are required to achieve algorithms by programming through teaching experiments and course exercise. Thus they can master the knowledge in terms of application. Putting the theory into practicability, the students can master the design method of cryptography algorithms and comprehend the important function of cryptography. After learning this course, they can have an entire view of cryptography.

Practical teaching should be optimized. There are integrated design experiment and an optional experiment in addition to the classical vertical experiments. The contents of practical teaching are list in table 3. The vertical experiments include classical cryptography algorithm (3 periods), DES algorithm (3 periods), RSA algorithm (3 periods) and implement of Elgmamal cipher (3 periods). The design experiment is achievement of RSA optimized algorithm (5 periods). The optional experiment is test of firewall.

Table 3. Practical teaching contents

Sequence Number	Practical teaching contents		
	Content	Period	Type
1	Implement of classical cryptography algorithm	3	Vertical
2	Implement of DES algorithm	3	
3	Implement of RSA algorithm	3	
4	Implement of Elgmamal cipher	3	
5	Achievement of RSA optimized algorithm	5	Integrated design
6	Test of firewall	Out of class	optional

At the beginning of practical teaching, all the students are divided into several groups; each group consists of three students, who should cooperate with each other to finish the experiments. In this way, the students can give full play to their subjective initiative and their ability of cooperating and innovative can be cultivated. Each group dispatches one person to report the results to the teacher, and the teachers check the work of others division at random After the class each student should write a detailed report according to the requirement of experiments and the content of experiment, the teachers instruct the students corresponding with their different levels. The students can select the optional experiment based on his actual condition, thus the students can apply adaptive learning. At the end, the teachers assess the score of student according the regular grade and experiment grade, encourage the students to be innovative through the assess process, and strengthen the students research ability.

Selection of textbook

Herein the characteristic of cryptography, and the practice and experience in teaching, take one textbook in priority and others for assistance in the selection of textbook. The chosen one should afford the foreland information and practicability, and probe the students to exert their activeness and format their own habit of thinking. Furthermore, it can apply to students of different levels, enable the value of knowledge can exert sufficiently. <Computer cryptography---data privacy and security in computer network>(3rd version) which is written by Kaicheng Lu and published by Tsinghua University Press, is chosen as the main textbook, it combines the development of cryptography in recent years, and introduces the basic principles and frequent algorithms of cryptography plainly, and strengthen the related contents of privacy security in network communication. Meanwhile, <Cryptography and Network Security: Principles and Practice> (4nd version) which is written by William Stalling, and < Introduction to cryptography: with coding theory > which is written by Wade Trappe and Lawrence C. Washington, are chosen to be the main reference books, because they are clear and comprehensible for students and they are of stronger practicality. In addition, other reference books are provided for students, such as < Cryptography and Network Security>(2nd version) which is written by Atual Kalate, <Applied Cryptography: Protocols, Algorithms, and Source Code> which is written by Bruce Schneier, etc..

Examine mode of cryptography

The characteristics of this course determines that its' examine mode is flexible and various. The students' final score is not only made up of their examination scores, but also made up of various norms. Assessing students' through various norms, only in this way can the students' integrate level of learning be assessed fully. The score is composed of four parts, the first one consists of the students' attendance and their performance of answering questions; the second one is the score of regular assignments of each student after class; the third one is the score that students obtained in practical teaching, the last one is the scores students obtained in their final examination. Students' final score can be calculated according to the corresponding portion of these four parts. The equation is as follows: The final score=attendance & performance (10%) +score of regular assignments (10%) +the score obtained in practical teaching (40%) +the score obtained in final examination (40%). Such examine mode can make the students not only pay attention to the knowledge in their textbook, but they also need to focus on their practical ability much more, and it can make sure that the students apply the theory they learned into the practice of solving problems, besides it can strengthen students' the innovative ability.

Conclusion

Cryptography is a basic course for computer science and technology major; this article mainly discusses the teaching method of this course.

This article designs the periods of theory and practical teaching, and it also designs the selection of textbook, as well as the examine mode of this course. All these lead to good teaching effect, and the students generally response that this course have cultivated their ability of innovation. It also affords certain reference value for same trade. In

nowadays society the development of computer network changes quickly, the teaching of cryptography should attach the corresponding importance.

REFERENCES

[1] Wang ChangJi, Liao DingFeng, and Huang HuaJie, "The Design and Analysis of Information Security Teaching and Learning Platform," 2009 First International Workshop on Education Technology and Computer Science, pp. 598602, March 2009.

[2] ZhongCheng, ZhaoYueHua, Introduction to Information Security, Wuhan University of Technology Press, 2003.

[3] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Publishing House of Electronics Industry, BeiJing, 2006.

[4] Cynthia Y. Lester, Frank Jamerson, "The Practice of Remote Education on Information Security," International Workshop of Innovation on Computer System Education, pp. 2609–2613, IEEE press, 2008.

[5] W. Hu, G. Wang, Q. Shi, T. Chen, Frank Jamerson, "Designing an Undergraduate Software Security Course," Secureware, pp. 257–262, October 2008.

[6] DOUGLAS Stinson Cryptography: Theory and Practice, CRC Press, 1995.

Authors: *Yi Sun, Lecturer, College of Information Engineering, Tibet Institute for Nationalities, Xianyang 712082, China. E-mail: outcasthgy@126.com; Jianmin Dong, associate Prof., College of Information Engineering, Tibet Institute for Nationalities, Xianyang 712082, China. E-mail: jmdong@189.cn; Hongwei Guo, Prof., College of Information Engineering, Tibet Institute for Nationalities, Xianyang 712082, China. E-mail: tuhw_guo@163.com; Liang Wang, associate Prof., College of Information Engineering, Tibet Institute for Nationalities, Xianyang 712082, China. E-mail: wzjwlwl@163.com; Zhaohai Ran, Lecturer, Network Information Center, Tibet Institute for Nationalities, Xianyang 712082, China. E-mail: rzjl@163.com.*