Reforming cryptography education by teaching practical sessions

Lina Zhang, Weiguo Zhang, Ninghong Zhu & Yanyan Jia

Xi'an University of Science and Technology
Xi'an, Shaanxi, People's Republic of China

ABSTRACT: The Ministry of Education in China, in launching a number of programmes on *outstanding engineering education and training*, is aiming to attract into the field a large number of high-quality engineers with innovative ability. Producing such well-qualified and skilled engineers is assisted by the type of practical teaching offered in engineering and technology education. The authors have analysed the course, Modern Cryptography, and have described in this article the new curriculum for this course, as well as the features, aims and issues associated with the course. Three measures of reform are discussed, such as training in practical ability, the teaching content and the assessment methods. The study carried out has shown that such reforms can achieve positive results. The measures proposed here could be used in engineering and technology education and practice to provide a reference model for teaching reform.

INTRODUCTION

Various universities, research institutes and enterprises in China have attached great importance to the Ministry of Education's Plan for Educating and Training Outstanding Engineers (PETOE), since it was proposed in 2010 [1][2]. They believe it is an important initiative in engineering education. In responding to the challenges raised by information security, China needs to cultivate a large number of outstanding engineers with international vision and a strong humanistic quality, as well as skills and abilities in science and engineering.

The Chinese Association for Cryptologic Research (or CACR), has organised several seminars on teaching information security. In fact, many colleges and universities are actively reforming the content and methods of teaching their courses on information security and cryptography; for example, the Beijing University of Posts and Telecommunications, Beijing Polytechnic University, Wuhan University and many other institutions. These reforms have been very successful. However, the nature and characteristics of these institutions are not all the same and their teaching methods are not identical.

Three specialty streams were run for undergraduate teaching by the School of Computing Science and Technology at Xi'an University of Science and Technology in 2012. Information security was one of the streams, and modern cryptography is one of the main courses. At present, this is a specialised course on information and computer science within the Institution; many other specialties are listed as compulsory or elective. In order to keep pace with developments, a break from the traditional system of teaching cryptography was proposed. The proposals were analysed and the content of the cryptography course updated to cultivate innovative skills and to conform to the requirements of PETOE.

The authors carried out a significant amount of preparatory work related to the practical teaching of cryptography; for example, the direction of the training programme, surveys on employment opportunities in information security and other areas. The reforms outlined in this article would also play a role in improving teaching of information security, as well as promoting the reform of other courses at the Institution.

ANALYSIS OF STATUS AND CHARACTERISTICS

The Ministry of Education's Plan is to train a large number of well-qualified engineers with the aim of building an innovation-oriented country. The School of Computing Science and Technology cultivates skills in information security. China's Higher Education Act aims to foster creativity in higher education. For the School and related cryptographic professional courses, innovative teaching is most important.

Traditional teaching of cryptography has many shortcomings and teaching reform is needed to meet the growing demands of society. There is too much emphasis on theory and too little on practical problem-solving. The course is mainly based on lectures, supplemented by PowerPoint or similar presentation tools. The practicals exercise traditional cryptographic mathematical principles and related verification algorithms. The practicals are relatively independent of each other, and are not realistic and, hence, do not cultivate hands-on skills relevant to a real environment.

The problems with the traditional teaching method are: first, the sessions are centred on the simple verification of theory, which does not require students to think beyond this; second, the content is compartmentalised with little interdisciplinary knowledge linking it to other courses; third, it does not extend students' abilities in research. After completing the course, some students still appeared to lack awareness of course content. Finally, the content is outdated and does not adequately reflect developments in science and technology.

THE NEW CURRICULUM

Modern Cryptography: Traditional Teaching

The Modern Cryptography course is a cross-disciplinary course, with broad content including mathematics, computer science, communications and information systems [3][4]. Modern Cryptography involves basic knowledge of mathematics and is taught after the fundamental (foundation) courses. Content of the precursor courses includes number theory, algebra, probability theory and computational complexity theory. Often, a precursor course would cover the mathematical basis of information security or introduce essential basics first before the actual cryptology course.

The fundamental purpose of cryptography is to protect information stored and transported on networks. Therefore, the course involves many branches of computer science, of which, software design and network communications are two examples. In addition, cryptography requires complex computations and large amounts of data and so must be implemented through software.

The Modern Cryptography course aims to stimulate students' enthusiasm and initiative; for example, it is better for students to start from the information security issues met in real life and use the knowledge learnt on the course to solve them.

Figure 1 displays the curriculum viewed as three layers. Layer 1, the core of the course, has five components. Students must understand these core elements, the concept of cryptography; and have a relatively clear and complete understanding. Layer 2 consists of various elective modules, which students choose for in-depth study. They are required to be familiar with the cryptographic algorithms, and understand encryption and authentication technologies. Layer 3 of the course is pursued by private study.

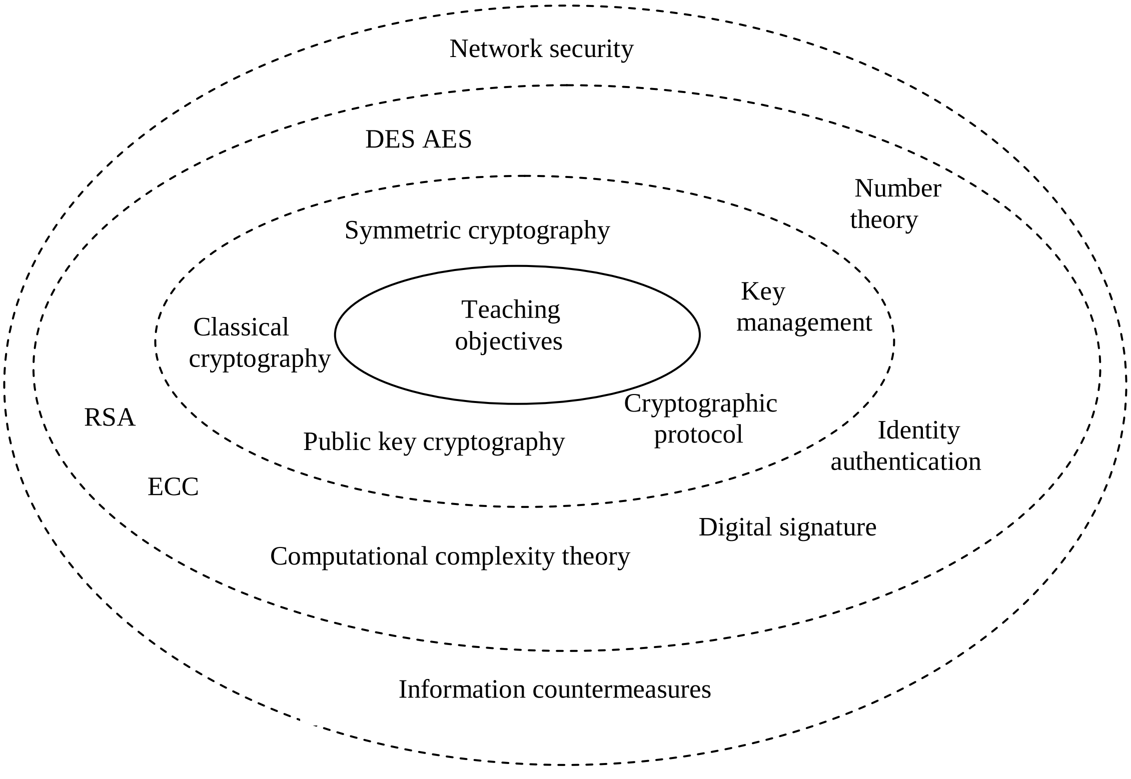

Figure 1: The curriculum structure.

MODERN CRYPTOGRAPHY: UPDATING THE COURSE

The Modern Cryptography course must recognise the different levels of students' ability. The following was implemented to improve the teaching.

First: multimedia courseware and demonstration were used to teach theory. Interest is the best teacher, and students' enthusiasm may be stimulated by simple demonstrations in class. For example, by analysing security issues that arise in on-line shopping, students could grasp the three fundamentals of cryptography: integrity, confidentiality and non-repudiation. These classical cryptographic concepts may be students' first contact with the subject, and some may still not fully understand the basic concepts. At this point, the teacher could let four people within each group role-play, i.e. two could be *communicating personnel*, and two could be *attackers* - people who attack the communicators. The communicating personnel use classical cryptography to communicate, while the attackers try to break the communication codes.

Second: the content of the course must be designed and updated to enhance, the students' enthusiasm. The practical content of the current course is relatively limited. The specific content is discussed below.

Third: the course should thoroughly train the students. For example, in the School at Xi'an University of Science and Technology a week is set aside for an experiment, such as a network transmission system using cryptography algorithms. In this system, there would be session keys, which are generated using random numbers, and the transmitted data would be encrypted by the symmetric encryption algorithm; the signing and verification functions would be completed using the public key cryptography algorithm. This model helps students to study cryptography. Students can write part of the program code themselves or choose to use a third-party code library. Students will encounter a variety of problems and inadequacies may surface in the design process. By re-examining progress, students can consolidate their knowledge.

Fourth: the school emphasises the practical nature of the student's graduation thesis or design. The graduation thesis is an important part of the undergraduate's training. It requires an in-depth understanding of communications and the completion of tasks, such as writing a paper. The teacher must cultivate the analysis and the problem-solving abilities of students, as well as the ability to work independently, be well-organised and have good communication skills. By combining the practical sessions and the graduate thesis, the student's abilities are improved aiding the transition from university to employment.

As well as a small number of validation practicals, a number of classical algorithms can be used during the practical sessions. This can stimulate students' interest and develop their programming ability. A variety of cryptographic algorithms are available for students to select from and implement. This type of practical teaching achieved good results in the graduation thesis component of the course. The overall effect has been to improve the students' attitude and is an improvement over the previous, traditional method.

The practical teaching includes a combination of demonstrations, *operational* experiments and *independent* experiments. The demonstrations were Flash presentations and *dynamic* presentations. Flash presentations provide a visualisation of abstract cipher algorithms, allowing students to develop an intuitive understanding. Dynamic presentations *explain* an algorithm in detail. Students can complete some of the work in their own time. This practical teaching not only improves the students' programming skills, it also helps them to think about the course content. There are many demonstrations and some of these could be taken out of class.

The operational experiments are designed to focus on the cultivation of students' practical ability and to encourage positive thinking. This can be illustrated through an example: the teacher selects a bank certification system for analysis while students complete exercises and presentations. The content of the session includes algorithm selection, generation of a public-key certificate, encrypted data transmission and a series of authentication steps.

The overall process helps students to gain a deep understanding of the various functions. Importantly, when designing such experiments, it is vital to focus on giving students a sense of fun and enjoyment while they tackle these tasks, and to help them find the pleasure that can be gained from studying successfully what are a large number of complex algorithms and operations.

The independent experiments are carried out through open teaching. For example, students choose cryptology-related topics according to their interest. Students are expected to provide a literature review, an experimental design, preparatory material and conduct the experiment. Teachers should ensure that students provide references [5], which can include Master's and doctoral theses, professional journals, international conferences papers and authoritative Web sites. By these means, students can learn of the latest developments and discover cryptographic points of interest.

Based on the ideas of engineering education, improving students' practical experience is important during teaching, as is the course content itself [6-8]. Teachers could boost students' enthusiasm by introducing open source software into the course and drawing on user experience, etc. The content of demonstrations and experiments is shown in Table 1.

Table 1: The content of demonstrations and experiments.

Experiments	Design and content
Demonstration experiments	Dynamic display of the detailed process of DES *(Data Encryption Standard)*, AES *(Advanced Encryption Standard)*, RSA *(from Ron Rivest, Adi Shamir, and Leonard Adleman)*, and ECC *(Elliptic Curve Crypto)*, etc.
Operation experiments	Classical cryptography *offensive* experiments; implement the symmetric encryption algorithm (DES, AES), Hash algorithm (SHA1, MD5) and design and implement the simplified RSA algorithm.
Independent experiments	The calculator for cryptography; the analysis of the bank's authentication system.

ASSESSMENT METHODS AND COLLABORATIVE DESIGN

Practical teaching improves students' skills. Therefore, it is appropriate to change course content to include more practicals. Practical teaching is also important in improving students' innovative ability and problem-solving skills. Due to the lack of supervision and assessments in the previous practical sessions, many students underestimated the value of classroom learning, and this impacted their practical abilities. To improve the quality of practical teaching, reform of the evaluation and supervision is necessary.

The assessment methods for the teaching of practical sessions were analysed for this study and reformed and are outlined here. The evaluation emphasises the importance of practical study and so an assessment is part of the experiments. The assessment is based on four aspects.

First: the students' collaborative work. The students need to strengthen co-operation within a group and learn how to share resources. Second: the implementation of the algorithm. Students still need to master the basic theory and improve their programming ability. Third: problem-solving and summarisation. The students must develop good study habits, and learn to summarise and analyse the problems they meet. Fourth: compare and contrast their implemented algorithms with popular alternatives. The assessment has four grades, viz. excellent, good, fair or poor.

CONCLUSIONS

Modern Cryptography has become a specialised course within the School of Computing Science and Technology. Over the years, teachers in the School have carried out much work to reform and reconstruct the teaching content and methods of the course. Modern Cryptography has distinct characteristics to meet the teaching and employment needs.

The course is based on ideas from engineering education and so, therefore, should have a rich content. The teaching has multiple forms and has improved greatly in recent years, in breadth and depth. The forms of assessment meet good academic standards. The students are highly participatory and enthusiastic about the course. There are many cryptology-related topics in the students' graduation theses, almost all of which are in-depth studies and well-executed. To reiterate, most students have high expectations of the course. It proves that this reform of content and practice can be considered successful. This approach could be extended to other specialised courses.

ACKNOWLEDGEMENTS

This work was supported by the Xi'an Science and Technology Project (No. SF1232-5).

REFERENCES

1. Chen, H., Tan, Z. and Yang G., Discussion on *outstanding engineers* training program for information security major in China. *Proc. Inter. Conf. on Future Computer Supported Educ.*, Seoul, Korea, 868-872 (2012).
2. Xu, W.D., Analysis of excellence engineer talent training model of newly built undergraduate course colleges and universities. *Meitan Higher Educ.*, 30, **3**, 57-60 (2012).
3. Wu, C.Y., Analysis on the information security education for the public security active forces academy. *Proc. Inter. Forum on Infor. Technol. and Applications*, Kun Ming, China, 355-357 (2010).
4. Zhang, R.X. and Yao, G., Research on cryptography teaching of information security. *China Modern Educational Equipment*, **1**, 159-160 (2011).

5. Jonathan, R.., Online education as a toll good: an examination of the South Carolina virtual school program. *Computers and Educ.*, 57, **2**, 1583-1594 (2011).
6. Li, W., The status and developing strategy of China's continuing engineering education. *Procedia Engng.*, 29, 3815-3819 (2012).
7. Zhang, Y.T. and Wang, S.Y., Continue to carry out the reform and developing strategy study of higher engineering education. *Higher Engng. Educ. Research*, 6, 9-14 (2005).
8. Chen, K., A preliminary study on the development models of continuing education for professional and technical personnel based on SNS. *Modern Educ. Technol.*, **6**, 41-45 (2010).