Universe Scientific Publishing

10.18686/ahe.v7i2.7092

Exploring the Integration of Civics Elements in the Teaching Reform of Cryptography Courses

Peng Luo, Chunming Zhang

Armed Police Engineering University, Xi'an, Shaanxi 710086

Abstract: In view of the current teaching practice of incorporating the element of thinking politics into professional courses, the basic idea of thinking politics in the curriculum is elaborated from six aspects based on the general requirements for the construction of thinking politics in science and technology courses as stated in the Guideline for the Construction of Thinking Politics in Higher Education Courses issued by the Ministry of Education, and the analysis of the characteristics of the core course of cryptography in cyberspace security.

Keywords: Cyberspace security; Cryptography; Curriculum thinking

In June 2020, the Ministry of Education issued the "Guideline for the Construction of Curriculum Civics in Higher Education Institutions", which specifies the specific objectives and contents of the construction of curriculum civics, and sets out the basic requirements for the teaching design of different types of courses and the teaching contents of different types of specialised courses. In this regard, specific requirements have been set out for the proper development of the ideology of science and engineering courses, i. e. to combine the education of Marxist positions and methods with the cultivation of the scientific spirit, and to improve students' ability to correctly understand, analyse and solve problems. In science courses, emphasis should be placed on the training of scientific thinking methods and the education of scientific ethics, so as to cultivate students' sense of responsibility and mission to explore the unknown, pursue the truth and climb to the peak of science. In engineering courses, emphasis is placed on strengthening students' education in engineering ethics, cultivating the spirit of national craftsmanship for excellence, and inspiring students to serve their country with a sense of responsibility and mission in science and technology.

As society becomes more and more computerised, various information security risks arise along with it. The international struggle for cyberspace security is intensifying, and the struggle for control of cyberspace security is a strategic high point. China has become a major cyber power, but due to the weak foundation of cyber technology and the lack of cyber security talents, China is not yet a strong cyber power.

In order to build a national information security system, the government, army, public security and other important national departments, as well as important infrastructures such as finance, electricity and energy, all need a large number of information security specialists.

Cryptography is a fundamental discipline for network information security, and if the cryptographic system needs to be changed, then the overall network information security involved will need to be adjusted accordingly. This is why cryptography is so important to cyberspace security[1][2].

Cryptography has the following characteristics compared to other university courses in science and technology: it covers a wide range of knowledge, it is a difficult course, and it has a strong theoretical and applied focus. The study of cryptography requires a number of pre-requisite courses, including number theory, modern algebra, mathematical operations on finite fields and network security protocols, depending on the focus of the curriculum. The pre-requisite courses are difficult, particularly as they require a high level of mathematical knowledge.

At the same time, the cryptography course itself covers a wide range of knowledge. In general, the course content often covers cryptographic fundamentals, classical cryptography, private key cryptography, public key cryptography, hash functions, digital signatures, authentication and identification, cryptographic applications in e-commerce, design and development of net-

work security protocols, and public key infrastructure. The wide range of knowledge makes cryptography a difficult course to teach and learn. Most students report that the course is too difficult to learn. This is why the course requires detailed derivation and analysis of the algorithms, as well as ways to make the course content more interesting and applicable in order to engage students. In addition, the course is characterised by a strong theoretical and applied foundation, and students are interested in the applications of cryptography in the course [8].

1. To cultivate patriotism in students

In the introduction to the cryptography course, you can talk about the relationship between cryptography and warfare, starting with the "Haomi", which is the most proud of the Chinese Revolutionary War, so that students can understand that it is with this high-level cryptography that the Party and the army can ensure the absolute security of wireless communication, and that they can plan in a tent and win in a thousand miles. For many years, MD5 and SHA-1, which are based on the hash function promulgated by the US National Institute of Standards and Technology (NIST), have been recognised as the two most advanced and widely used algorithms in the world. These two algorithms are powerful in that any small tampering with the input information immediately causes an "avalanche effect", thus ensuring that the digital fingerprint of the information is unique and cannot be forged. As a result, it would take a million years of computing to crack it, even with a large computer. However, the two most secure cryptographic algorithms in the world were cracked by Wang Xiaoyun in 2004 and 2005, shocking the international cryptographic community. Most importantly, most of her work on these two algorithms was done on ordinary computers and with hand calculations. Her work also led to the phasing out of MD5 and SHA-1 hash functions from almost all software systems in industry[3]. After the two pillars of the hash function had been hit hard, in 2007, the National Institute of Standards and Technology (NIST) invited cryptographers from all over the world to design a new international standard cryptographic algorithm. This section can be shown in the form of a short film, which combines sound and images to instil a sense of national pride in the students.

2. Enhancing students' sense of mission to serve their country through science

In introducing the course content, students will understand that modern cryptography and many mathematical theories were established in the West. Looking back on our modern history, the Chinese people have suffered and sacrificed so much that it is unprecedented in the history of the world, and one of the roots of our backwardness and defeat is our backwardness in science and technology. As the war raged on, many intellectuals realised that "if China is to be strong, it can only rely on the strength of the Chinese themselves". In the face of suffering, they rose up and fought, and finally, under the leadership of the Communist Party of China, set out on the right path to achieve national independence and liberation, and found the broadest stage in life to serve their country with science. A generation has its own struggles. Whether it was Su Buqing, Huang Weilu, Cheng Kaijia, Zhu Guangya, or Tu Youyou, Yuan Longping, Huang Xuhua, Huang Da, the spirit of scientists has long been embedded in the bloodline of generations of Chinese scientists and has been passed down through time and space. With a strong sense of patriotism, these outstanding intellectuals, with their profound academic attainments and broad scientific perspectives, have made significant contributions that have gone down in history, reflecting their noble character and excellent style of learning.

3. Educating about the ethics of science

The security of a cryptographic system depends on the weakest link in the system - the "barrel theory"[5] - and the best technology is meaningless without effective management. This is why it is important to strengthen the management and training of security personnel. Computer technology is a double-edged sword, and whether it can benefit or harm mankind depends on the moral awareness of the person who wields it. It is also about helping them to develop a correct outlook on life, the world and their values, and helping them to see life's problems in a proper way, and to recognise their own abilities and values and give them a sense of social identity. According to Maslow's theory, the needs of computer technology owners should be met in terms of dietary needs, self-protection and social protection, team integration, recognition and self-fulfilment. One of the most important ways to prevent IT professionals from committing crimes is to make the content of the civic ethics programme a central part of the promotion of online ethics, and the relevant education departments should include computer ethics education in the scope of general moral education, so that people can develop a correct moral outlook by improving their ability to distinguish between right and wrong [4].

4. Educate on engineering ethics

The Enigma cipher machine can be used to teach engineering ethics when explaining the principles of classical crypto-

graphic equipment construction. The Enigma cipher machine designed by German engineer Arthur Scherbius was so secure that it could not be deciphered by an enemy who did not also have the key to the three lines of defence. During World War II, the Enigma was used as the standard cipher from the German General Headquarters down to the army, navy and air force [6-8]. It can be said that the Enigma cipher machine was an important milestone in the history of cryptography, but instead of benefiting mankind, it helped the German fascists to commit their heinous crimes. In contemporary society the goals of engineering practice can easily be equated with the growth of commercial interests, and this has been criticised by society as more and more projects are carried out. There is a growing recognition of the power that engineers have through the application of modern science and technology, which requires them to take on more ethical duties and responsibilities. From the point of view of human development, information security practitioners emphasise the professionalism and independence of the profession and the need to strengthen professional ethics. From the point of view of engineering practice (project development), good engineering must bring more convenience to society, and the ethical issues in engineering practice in the social context must be taken into account in the construction of the curriculum.

5. Training a scientific way of thinking

Scientific thinking is one of the core literacies of cyberspace security, and is an important way to develop scientific methodology. Many important concepts and laws are the product of scientific thinking, and the formation of scientific thinking needs to be accomplished through the continuous formulation and solution of problems, so the design of timely, appropriate and moderate problem strings in classroom teaching can effectively cultivate and develop students' scientific thinking[9]. For example, when explaining the background of the public key cryptosystem, students can briefly describe the basic principles of symmetric cryptosystems such as group ciphers and sequence ciphers, and be guided to consider that the keys used by both encryption and decryption parties are secret and need to be changed periodically, and that new keys are always distributed to the users through some secret channel. It is therefore limited by the problem of securing the exchange of keys between the two communicating parties. In addition, if a trading party has several trading relationships, he has to maintain several special keys. It is also impossible to identify the originator or the end-user of a trade, because both parties to the trade have the same key. Furthermore, as symmetric cryptography can only be used to encrypt and decrypt data, providing confidentiality, it cannot be used for digital signatures. There is an urgent need to find new cryptographic systems.

The scientific way of thinking can be applied not only in the professional world, but also in everyday life. It helps students to think more rationally and to solve problems effectively. Teachers guide students to think deeply, so that they can develop good behavioural habits, good qualities, a correct outlook and a healthy personality. At the same time, teachers should cultivate students' scientific research spirit of being bold and innovative, and encourage them to actively innovate and serve the national economy with information security-related technologies.

6. Cultivating the spirit of a great craftsman for excellence

When teaching sophisticated cryptographic algorithms such as DES and AES, students are encouraged to develop the spirit of craftsmanship. All countries in the world that have developed manufacturing industries place great importance on the cultivation of craftsmanship. The spirit of craftsmanship is the spirit of the craftsmen and women who work on their products, such as seriousness and dedication, a sense of quality, perseverance and a sense of fame and fortune. Not only is craftsmanship needed in production and construction, but also in scientific research[1].

Scientific research is a noble pursuit of truth and the revelation of laws, requiring a high degree of responsibility and dedication. Surveys of the world's most distinguished people in various fields have shown that, with serious and responsible dedication, one can achieve extraordinary results even if one is not in one's favourite or most desirable position. The same applies to scientific research. Only by taking an extremely responsible and serious approach to the work we do will we be able to make discoveries and breakthroughs on the road to the unknown.

Only by being meticulous and striving for excellence can we polish the best. Only by abandoning the mentality of "maybe", "perhaps" and "almost" can we build a tower of victory on a solid foundation. Many of my predecessors in the cryptography field have often worked word by word to complete a high-quality academic article.

The text was discussed and revised again and again, sentence by sentence, until it was found to be free of any problems before publication. This shows that only by adhering to high standards and strict requirements, by thinking through every aspect and detail, is it possible to achieve the highest level of quality [10].

In scientific research there are more failures than successes, and "nine lives to die" is the norm. It is only through perse-

verance in the day-to-day, trivial and tedious process of research that we can reach the end of the road. Looking back on the history of scientific research, it is easy to see that the so-called lightbulb moments are often the result of years or decades of perseverance and dedication.

7. Conclusion

In order to implement the fundamental task of educating people through moral education, it is necessary to integrate the shaping of values, the imparting of knowledge and the cultivation of abilities, which cannot be separated. To comprehensively promote the construction of curriculum thinking and politics is to integrate the guidance of values into the teaching of knowledge and the cultivation of abilities, and to help students develop a correct world view, outlook on life and values, which is a proper and necessary part of talent cultivation. As a core course of the cyberspace security major, the cryptography course, under the guidance of the concept of "Thinking Politics in the Curriculum" and the "Guideline for the Construction of Thinking Politics in the Curriculum of Higher Education Institutions", will continue to improve the level of talent cultivation by exploring the elements of thinking politics in the curriculum, so as to cultivate students into innovative talents with solid professional knowledge and firm beliefs.

References

[1] Yang Hua. Education also needs craftsmanship [J]. Curriculum Education Research: Studies on Learning and Teaching Methods, 2018(13): 119-119.

[2] Li Yanjun, Ou Haiwen. Research on the construction of quality courses in cryptography in special institutions [J]. Journal of Beijing Institute of Electronic Science and Technology, 2020, 28(3): 74-80.

[3] Wang Dangwei. The construction and application path of "course thinking politics" in the professional background course group of military schools [J]. Journal of Air Force Early Warning College, 2021, 35(03): 221-224.

[4] Pan Meng. Ethics and morality in scientific research of network information security An analysis [J]. Digital World, 2019(06): 244-245.

[5] Guo Yuyan, Jiang Mingming, Xiao Jianyu, Sun Mei. Exploring the construction of information security courses under the perspective of curriculum thinking and government [J]. Journal of Langfang Normal College (Natural Science Edition), 2021, 21(02): 100-103.

[6] Dou Bennian, Xu Chungen, Jin Xiaochan. Humanities education in cryptography courses[J]. Computer Education, 2019(03):1-3.

[7] Jia Zhongtian, Liu Yue, Zhang Bo. Exploring the experience of network attack and defense course construction [J]. Computer Education, 2019(03): 12-15.

[8] Jia Weifeng, Yang Libo. The characteristics of cryptography and its teaching methods [J]. Journal of North China Institute of Water Conservancy and Hydropower (Social Sciences), 2010, 26(03). 169-170.

[9] Li Jin, Cao Jin, Zhang Yueyu, Zhang Meiru, Li Hui. Reverse teaching design of information security professional course Civics - taking "Wireless communication network security" course of Xi'an University of Electronic Science and Technology as an example [J]. Journal of Network and Information Security, 2021, 7(03): 166-174.

[10] Hu Aijun, Li Guyue, Peng Linning, Li Tao. Exploring the teaching of frontier technologies of cyberspace security integrated with Civics [J]. Journal of Network and Information Security, 2019, 5(03): 54-66.