Scientific and Social Research
2022, Volume 4, Issue 8

Teaching Exploration and Practice of Integrating into Ideological and Political Education in the Course of Technology of Applied Cryptogram

Xiaoming Hu*, Chuang Ma

College of Computer and Information Engineering, Shanghai Polytechnic University, Shanghai 201209, China

***Corresponding author:** Xiaoming Hu, xmhu@sspu.edu.cn

Abstract: This paper summarizes and classifies the teaching contents of technology of applied cryptogram course according to the knowledge points. At the same time, the ideological and political elements of the course are designed from the following perspectives; (1) Abiding laws and regulations, and using cryptographic technology for the protection of network security; (2) Enabling students to firmly establish the belief that "core technology should be independent, and China's science and technology should be self-improvement." Further, the ideology and political elements are integrated into different teaching contents according to the knowledge points around these two themes. This course balances the relationship among ideology and morality, knowledge ability and quality. It not only focuses on improving students' learning interest and ability, but also cultivates students to establish the correct outlook on life and values. The practical application shows that the overall effect is good.

Keywords: Ideological and political education; Technology of applied cryptogram; Cryptography; Teaching method

Online publication: August 12, 2022

1. Introduction

With the rapid development of network technology, problem in the network security has become more prominent. As one of the core technologies in solving the problem of network security, cryptography plays a very key role in solving problems-related to the network security [1-3]. However, cryptographic technology is a double-edged sword, where it can protect network security, and simultaneously it can bring great security risks and threats to the network. For example, encryption can help users protect confidential data, such as, personal documents and photos. Therefore, encryption is generally benign. However, when encryption is used by malicious attackers, it will cause very serious consequences to individuals, even society, and country, and the most typical way of malicious attack using encryption are blackmail virus [4]. Blackmail virus encrypts files with various encryption algorithms, and the infected people generally could not decrypt the files, and they should get the decrypted private key before they can decrypt them. Therefore, the hackers did not unlock the victim's files until they paid a certain amount of ransom. For example, on May 7, 2021, the Colonel pipeline transportation company, a large US product oil pipeline system operator, had to temporarily shut down their equipment, because the hackers controlled the computer system and data through illegal software, causing great losses to the company.

Cryptography is a core technology to achieve information security [5-7], and the effective use of cryptography is the key to information security risk control. The technology of applied cryptogram course

is a professional technical course with strong theory and technology in the network security course module of the network engineering major in the university. In the whole teaching process of technology of applied cryptogram, it is particularly important to integrate the ideological and political content into the teaching process. The ideological and political content is integrated into each module of the course through cases and other methods, with balance relationship between ideology and morality, knowledge and ability, and quality. On the basis of cultivating students to establish a correct outlook on life and values, focus should be given on improving students' learning interest and ability. Through courseware, test question bank, exercise guidance, cases, and other forms, promote students to master various knowledge and application skills of cryptography, and constantly adapt to the requirements of the society on network security professionals.

2. Integration design of ideological and political elements

The technology of applied cryptogram course carries out ideological and political design from the following two perspectives;

(1) Comply with laws and regulations, and use cryptogram technology for network security protection. Cryptogram technology is a double-edged sword, which guides students' honest, trustworthy, healthy, and civilized network behavior, improves students' network security awareness and level, and promotes the dissemination of socialist core values. In addition, it guides the students to abide by laws and administrative regulations, respect social morality, abide by business ethics, be honest and trustworthy, do not apply the learned cryptogram technology in network illegal and criminal activities, perform network security protection obligations, and maintain the integrity, confidentiality, and availability of network data when carrying out business and service activities.

(2) Enable students to firmly establish the belief that core technology should be independent, and Chinese science and technology should be self-improve. The development history of cryptography is relatively short, and there are still many key theories and technologies to be further studied and improved. By letting students understand the development, current situation, and mainstream technology of cryptography, students can firmly establish the belief that core technology should be independent, and Chinese science and technology should be self-improve, and cultivate students' awareness of scientific and technological innovation.

This course integrates ideological and political elements into the teaching content based on these two topics. The teaching content of the course includes the basic concepts, basic principles, and calculation methods of security, classical, and modern cryptography, hash function, key management, Commercial Cryptography, its classical algorithms, and cryptographic application in various industries. Each part integrates the corresponding ideological and political elements of the cryptography course, according to the knowledge points. The specific design is shown in **Table 1**.

Table 1. Mapping of knowledge points to ideological and political content and design of course

Knowledge unit (Chapter)	Course Ideological and political content and design
Fundamentals of cryptography and classical cryptography	This paper introduces the development history of cryptography. The use of cryptography is a double-edged sword, which enables students to increase their legal awareness and limit the research and application of technology to the cage of national laws.
Symmetric cryptosystem and asymmetric cryptosystem	Through some cases, it is analyzed that some cryptographic technologies have potential security risks, which will lead to serious consequences. Students should be guided to carry out independent innovation. In addition, core technologies should be independent and improve their innovation awareness.
Hash functions, message authentication, digital signatures, and key management	By introducing the design process and security analysis of hash function, students not only master the working principle of hash function, but also can analyze through examples, in which Professor Wang Xiaoyun broke through MD5, which shocked the world, and enhanced students' national pride and honor. In addition, introducing the Chinese commercial cryptographic algorithms independently developed by China, can make the students to appreciate the vitality of China's scientific and technological innovation.
Typical applications of cryptography in various industries	Through the typical application cases of cryptography in various industries such as, ID card and social security card, as well as the explanation of its double-sided nature, students can increase their legal awareness, limit the research and application of cryptography technology to the cage of national laws and apply what they have learned, and cultivate their ability to innovate and solve problems. Identity cards and social security cards are related to people's livelihood; therefore, the students can understand the importance of independent innovation in the core areas.
Experiments	Through experiments, the students can further strengthen their theoretical knowledge of cryptographic technology and have a certain understanding and mastery of its practice. Educate students can apply the theoretical and practical knowledge of cryptography to ensure national economic operation and improve people's living standards, and also guide the students to abide by laws and regulations.

3. The practice of curriculum ideological and political contents

Hash function [8-10] is one of the core technologies that is involved in cryptography. We should take a hash function as a practical example. Through the construction of hash function and the detailed explanation on how to be cracked, as well as causing a sensation in the world, students' sense of national pride is enhanced. At the same time, combined with SM3 hash function independently developed by the country, encourage the students to firmly establish the ideology of "core technology should be independent, and Chinese science and technology should be self-improvement." The specific practical design is shown in **Table 2**.

Table 2. Teaching process design of "hash function" with ideological and political elements

Knowledge unit (Chapter)	Teaching form	Teaching process	Ideological and political content
Hash function	Teaching	(1) Import; Analyze network security cases and events, and introduce the content of this lesson. (2) Course content; Hash function (case and heuristic teaching). (3) Ask questions; students think and find solutions (heuristic teaching). (4) Summarize and introduce the next lesson.	The hash function is a very important technology in cryptography. Currently, the mainstream algorithms used in the product are MD5 and SHA-1, which are not independently developed in China. In 2004, Professor Wangxiaoyun of China broke through MD5, and caused a sensation in the world. Our country independently designed SM3 hash function, subsequently stimulate students' democratic pride and cultivate students' ideological awareness of independent innovation.

This knowledge unit is taught by combining case and heuristic teaching. As shown in **Figure 1**, this method is used to further strengthen the understanding of the working principle and design of hash functions, and imperceptibly carries out ideological and political education. Other knowledge units can also refer to this method.

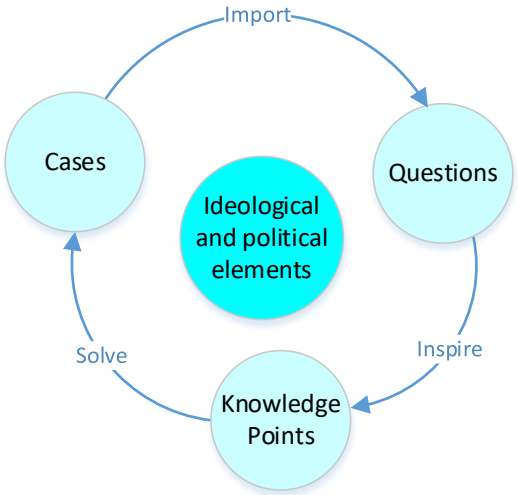

Figure 1. Teaching method design of "hash function" with ideological and political elements

4. Conclusion

This paper designs on how to integrate the ideological and political elements into the professional knowledge of the course of technology of applied cryptogram, and practices it through the hash function. Through practical application, it is found that it not only promotes students' mastery of various knowledge and application skills of cryptography, but also enables students to obtain positive energy and ability training from the classroom, such as, innovative thinking and consciousness, thereby students can firmly establish the belief of "core technology should be independent, and Chinese science and technology should be self-improvement." At the same time, improve students' enthusiasm and interest in professional courses. In addition, we should cultivate students' professional ethics and outlook, further establish correct network ethics, abide by laws and regulations, and use cryptogram technology for the protection of network security.

Funding

This work was supported by the Key Disciplines of Computer Science and Technology of Shanghai Polytechnic University, the Cultivation of Innovative talents-Construction of Curriculum System-Electronic Information, the Collaborative Innovation Platform of Electronic Information Master of Shanghai Polytechnic University, the First Class Undergraduate Specialty "Network Engineering" Construction in Shanghai (Project number: A30NH221903-0305), the Course Ideological and Political Navigation Plan of Shanghai Polytechnic University.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Yan G, 2021, Application of Information Encryption Technology in Computer Network Security. International Journal of Computational and Engineering, 6(4): 126-128.

[2] Yi Z, Jianhua F, Xiaoxin C, et al., 2021, Machine Learning Aided Key-Guessing Attack Paradigm Against Logic Block Encryption. Journal of Computer Science and Technology, 36(5): 1102-1117. https://org.doi/10.1007/S11390-021-0846-6

[3] Aghili SF, Sedaghat M, Singelee D, et al., 2022, MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. Future Generation Computer Systems, 131: 75-90. https://org.doi/10.1016/J.FUTURE.2022.01.003

[4] Xin Z, Xiaoling, 2022, Thoughts on Vulnerability Security by Ransomware Virus. International Journal of Social Science and Education Research, 5(1): 120-124. https://doi.org/10.6918/IJOSSER.202201_5(1).0019

[5] El AS, Lozi R, Puech W, 2022, Special Issue on Cryptography and its Applications in Information Security. Applied Sciences, 12(5): 2588-2591. https://org.doi/10.3390/APP12052588

[6] Galdi C, Kolesnikov V, 2022, Special issue: Security and Cryptography for Networks-SCN 2020. Journal of Computer Security, 30(1): 1-2. https://org.doi/10.3233/JCS-219000

[7] Guru A, Ambhikar A, Cardenas AA, et al., 2021, A Study of Cryptography to Protect Data from Cyber-crimes. Research Journal of Engineering and Technology, 11(2): 45-48.

[8] Yijun Y, Fei C, Zhiwei S, et al., 2019, Secure and Efficient Parallel Hash Function Construction and Its Application on Cloud audit. Soft Computing, 23(18): 8907-8925. https://org.doi/10.1007/s00500-018-3489-y

[9] Yousef AH, Mohamed FI, 2019, Reducing Hash Function Complexity: MD5 and SHA-1 as Examples. International Journal of Mathematical Sciences and Computing, 5(1): 1-17.

[10] Yuan Q, Tibouchi M, Abe M, 2022, On Subset-Resilient Hash Function Families. Designs, Codes, and Cryptography, 2022(90): 719-758. https://org.doi/10.1007/s10623-022-01008-4