Journal of Technology and Social Science (JTSS)

Development of Teaching Materials for Cryptography at Senior High School

Kenji Yamaguchi[1, a,*], Anna Kuwana[2, b] and Katsuhisa Kagami[3, c]

[1] Science & Education Center (SEC), Ochanomizu University (Ochanomizu University Senior High School), 2-1-1 Ohtsuka, Bunkyo-ku, Tokyo 112-8610, Japan

[2] Faculty of Science and Technology, Gunma University, 1-5-1 Tenjin-cho, Kiryu City, Gunma 376-8515, Japan

[3] Ochanomizu University, 2-1-1 Ohtsuka, Bunkyo-ku, Tokyo 112-8610, Japan

* Corresponding author

[a]<yamaguchi.kenji@ocha.ac.jp>, [b]<kuwana.anna@gunma-u.ac.jp>, [c]<kagami.katsuhisa@ocha.ac.jp>

Keywords: information education, common key cryptosystems, public key cryptosystems, teaching materials, Web applications

Abstract. We are engaged in the development of teaching methods and materials for information and mathematics in secondary education. In this education program, we develop teaching materials for cryptography. Cryptography is a very interesting subject area that uses information as well as math knowledge and skills. In this paper, we will provide an overview of cryptography, the actual situation in the field of education, and the application under development.

1. Introduction

In a highly information-oriented society, maintaining the safety of confidential information such as personal information is important. Cryptography, which consists of encryption processes and decryption processes, with keys (numbers) used in each process, is used to ensure security. Cryptography is classified as "common key cryptography" or "public key cryptography." In common key cryptography, the same keys are used for the encryption and decryption processes. The Caesar cipher used by Julius Caesar in ancient Rome is considered the beginning of common key cryptography [1]. The underlying method of public key cryptography was announced by Diffie and Hellman [2]. Moreover, Rivest, Shamir, and Adleman (RSA) cryptography, a public key cryptography method, was created by Rivest, Shamir, and Adleman [3]. In this type of cryptography, a public key is used for encryption, and a private key is used for decryption. The security of RSA cryptography depends on the difficulty of prime factorization, i.e., mathematical theory that guarantees the security of cryptography. These methods can also be combined in a method referred to as hybrid cryptography. For example, encrypted communication used in Internet shopping is referred to as SSL/TLS (Secure Sockets Layer/Transport Layer Security) [4], and SSL/TLS uses a hybrid cryptography method.

These are learned as knowledge in high school information classes. However, in many cases, they only learn the names of some cryptographies without knowledge of mathematical theory. In particular, proving the security of cryptography requires mathematical theory studied at the university level. Proving the security is difficult in the current situation.

Currently, high school students take either "Society and Information" or "Science of Information" classes in the subject area of Information. Each subject consists of 2 credits. However, in the new guidelines of study that will be started in high school in 2022, students will take "Information I" and "Information II." The former is a required subject, and the latter is an elective course. Each subject also consists of 2 credits. With the advent of high-level subjects such as "Information II," the subject

of information becomes increasingly important. In "Information II," students will learn about the flow of information, the mechanism of information processing as well as methods and technologies to ensure information security in information systems.

To solve these problems, we developed teaching materials which explain the mathematical theory that guarantees the security of cryptography [5]. They are designed to be easy-to-understand manner even for junior and senior high school students. The purpose is to gain an understanding of the importance associated with cryptography in the highly information-oriented society and the mathematics employed. If students enter numbers and letters in encryption and decryption processes on the Web application, these students will become interested in cryptography. In the following, we show the prototype development of the application that assists the mathematical understanding of Caesar cipher and RSA cipher, and the results of the questionnaire after the lesson.

2. The Goal of This Development

The Ministry of Education, Culture, Sports, Science and Technology (MEXT) has made available educational materials for teacher training for "Information I" and "Information II" on its website [6].

Consider the position of the cryptography in MEXT's educational materials. "Information I" consists of the "Information Communication Network" and "Data Utilization" sections. An item of encryption is present, and the name of the encryption method and encryption algorithm is mentioned. However, the mathematical principle of the actual algorithm is omitted. Individual cryptographic techniques such as RSA cryptography, elliptic curve cryptography [7–8], and SSL/TLS are mentioned in the "Information II" sections. The mathematical principles are omitted here as well. Our teaching materials are developed to compensate for these omitted parts. We develop the applications that explain Caesar cipher, RSA cipher, and Burnham cipher, within the range of mathematics that students can understand.

3. Prototype of the Teaching Materials

Figure 1 shows a prototype of the teaching material that helps students to learn the Caesar cipher. The prototype is implemented in Excel, but Web apps that can be run in Web browsers will be developed in the future.

As the sender, students can freely set the alphabet that they want to send to the other party and input this alphabet in (A). Afterward, the key number for encryption is freely set and input in (B). The key for encryption in the Caesar cipher determines the number of alphabet characters that will be changed. The encryption mechanism is explained in (C). Students can learn how to obtain the character code of encrypted text by adding the number of the key (B) to the character code of the plaintext inputted in (A). The encrypted character string is displayed in (D).

The students then learn the decryption of the ciphertext as the recipient who received the encrypted character. Moreover, the received character string is input in (E), assuming that (D) is received. Caesar cryptography is a common key cryptography, and hence the recipient also receives the key from the sender and inputs this key in (F). The mechanism of decryption is explained in (G). Students can learn how to calculate the plain code by subtracting the key from the character code in the reverse procedure of (C). (H) represents the original alphabet and here, should be the same as (A).

If the character code of the *i-th* alphabet in plaintext is $\mathrm{Code}(P_i)$, the key is K, and the character code of the *i-th* alphabet in ciphertext is $\mathrm{Code}(C_i)$, encryption can be expressed by Eq. (1) and decryption by Eq. (2).

$$\mathrm{Code}(C_i) = \mathrm{Code}(P_i) + K \quad (1)$$

$$\mathrm{Code}(P_i) = \mathrm{Code}(C_i) - K \quad (2)$$

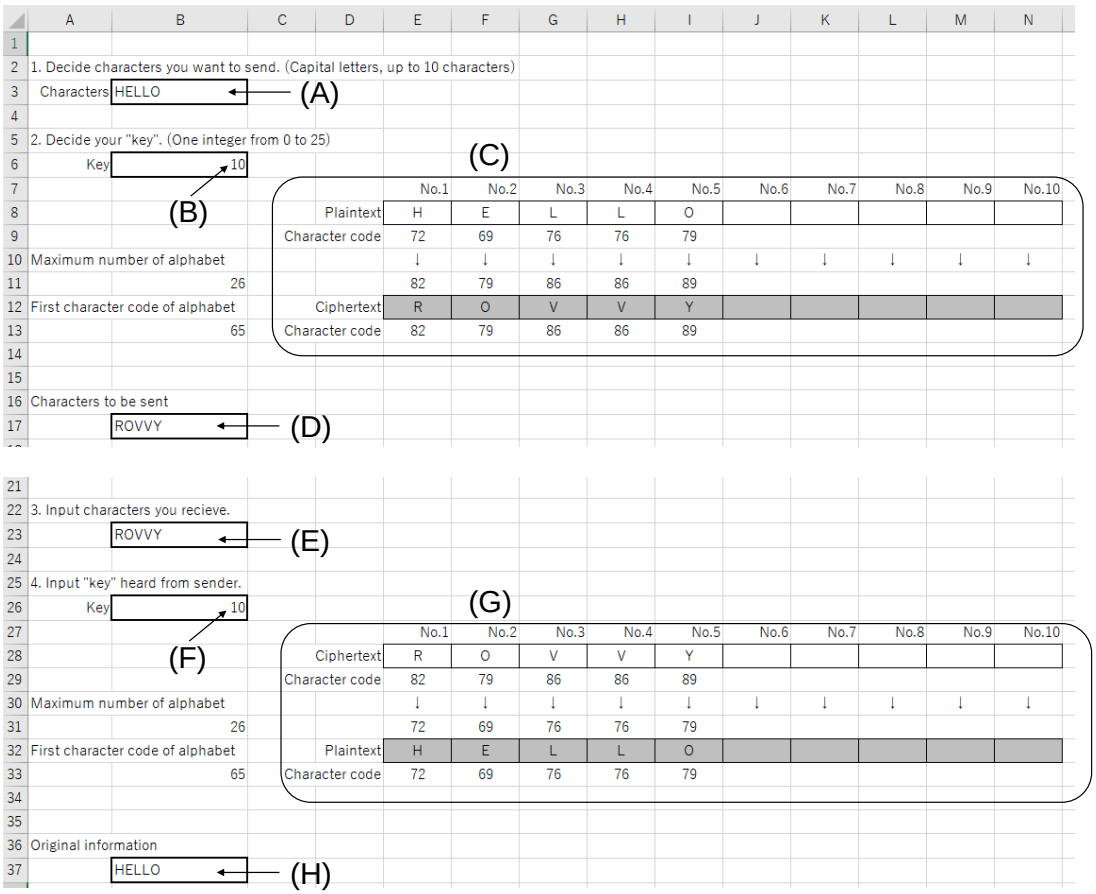


Fig. 1. A prototype of the teaching material used to learn the Caesar cipher.

Caesar cipher is a good topic to start the cryptography class in high school because of its simplicity and ease of understanding. However, it is not a secure cipher as it can be easily decrypted by trying all shift. On the other hand, RSA cryptography is a highly secure cipher that takes advantage of the complexity of prime factorization. Needless to send the key to the recipient is also the advantage of RSA cryptography.

Figure 2 shows the RSA cryptographic materials. Alice, the recipient, selects the prime numbers p and q as private keys and inputs these numbers in (I). Excel will calculate Alice's first public key N from Eq. (3) and display this key in (J).

$$N = p \times q \tag{3}$$

In addition, Alice determines e (where the greatest common divisor between $(p-1)(q-1)$ and e is 1), which is displayed in (K) and used as the second public key.

As the private key used for decryption, d is calculated from Eq. (4) and displayed in (L).

$$\mathrm{mod}(ed, (p-1)(q-1)) = 1 \tag{4}$$

The modulo operation $\mathrm{mod}(X, Y)$ returns the remainder of a division, after X is divided by Y. Bob, the sender, inputs the number he wants to send Alice in (M). Imagine that in the real world this is (for example) a character code or digitally represented music, movie, or picture. Using Alice's public key, c is calculated from Eq. (5) and displayed in (N). c represents the encrypted information and is given as follows:

$$c = \mathrm{mod}(m^e, N) \tag{5}$$

Upon receiving (N), Alice can calculate using her private key d and Eq. (6) to determine the information (O) that Bob wanted to send. This should be equal to (M).

$$(\mathrm{O}) = \mathrm{mod}(c^d, N) \tag{6}$$

Similarly, we developed the material that can teach a simple substitution cipher and a Vernam cipher. The details are omitted here.

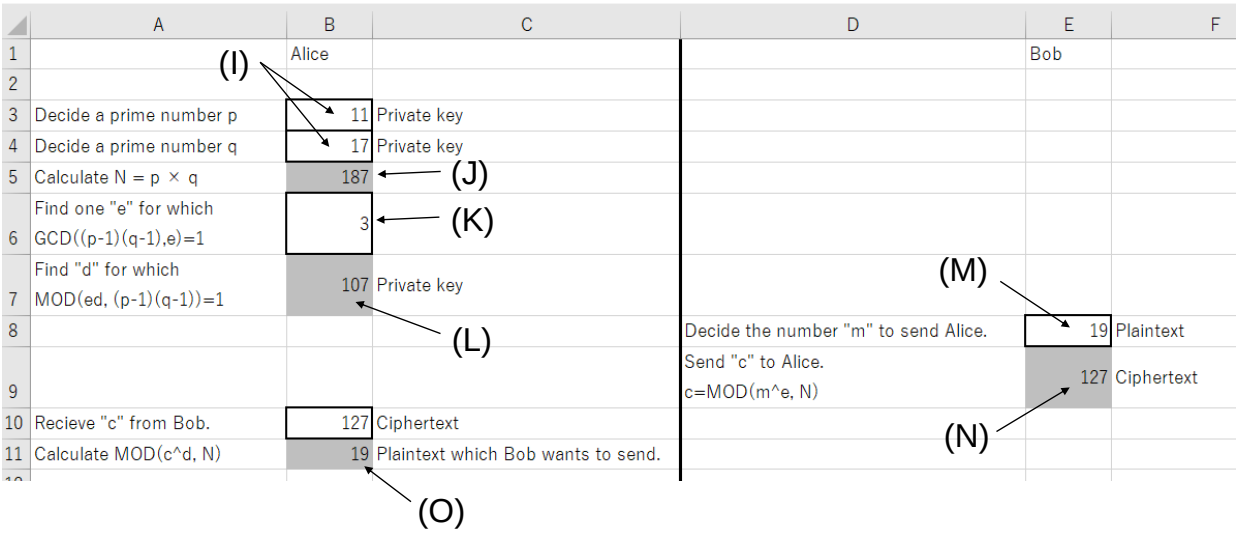
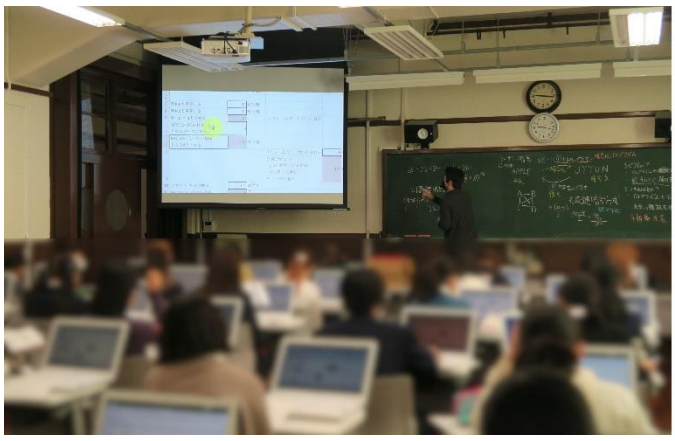


Fig. 2. A prototype of the teaching material used to learn the RSA cipher.

4. Practice in High School Class

One hundred and twenty first-year high school students in Japan (40 students, 3 classes, Ochanomizu University Senior High School) participated in a cryptography class using prototype teaching materials. As shown on the left in Fig. 3, the teacher explained the mechanism and principle of cryptography using a blackboard. Students understood how cryptography works by filling out the distributed worksheets as shown on the right in Fig. 3. Then, students input numbers and letters into the prototype of the teaching materials and tried encryption from plaintext to ciphertext and decryption from ciphertext to plaintext. Students also tried to receive the ciphertext encrypted by another student and decrypt it into plaintext.

Figure 4 shows a co-occurrence network from impressions written by the students after class. This network was developed by KH Coder [9]. Many students think “RSA is difficult,” and therefore we will improve the teaching material shown in Fig. 2. As an improvement plan, we are thinking of creating an interactive GUI, giving a detailed explanation, and exemplifying the numbers to be entered.



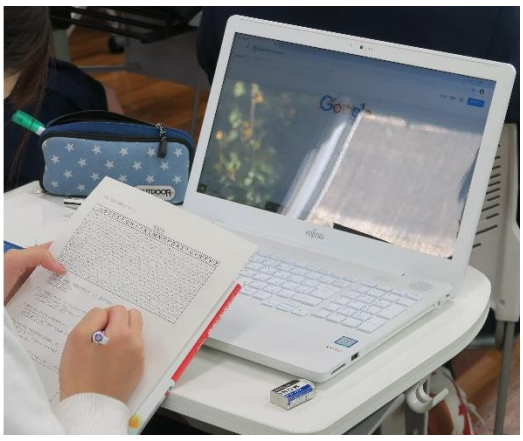


Fig. 3. A class (the photo is blurred in consideration of student's personal information).

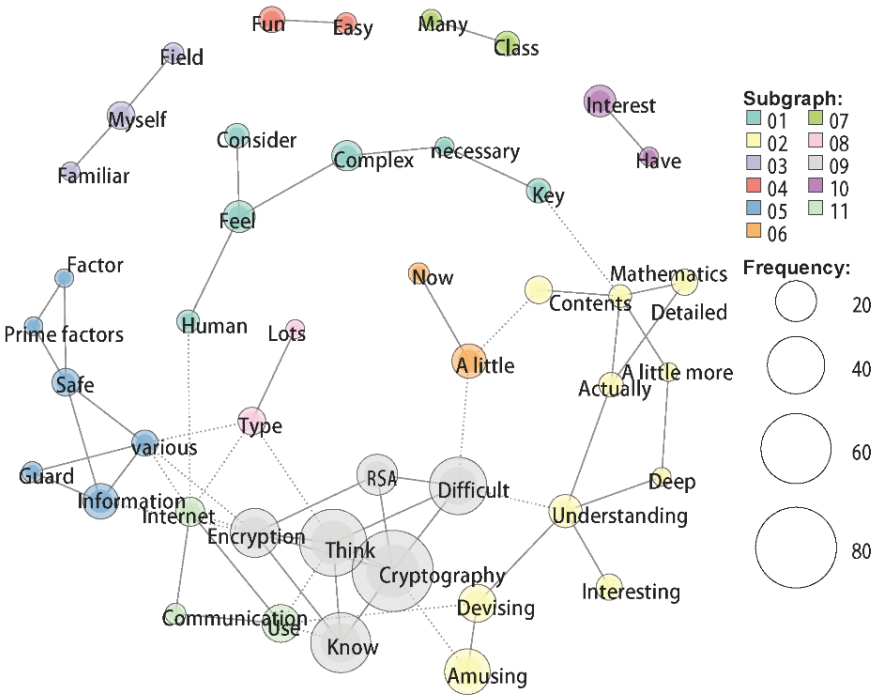


Fig. 4. A co-occurrence network from impressions written by the students after class.

5. Conclusion

We introduced the cryptographic learning application under development and introduced the impressions of students in high school classes using this development. In the future, we plan to implement this application as a Web application and publish the application with a teaching plan to enable easy use by teachers from other schools. The student who acts as an eavesdropper should be provided by a text encrypted by another student. By trying decryption, students can learn the strength of encryption.

Acknowledgments

We gratefully acknowledge the support of the new educational program development project for educating women in science at the schools attached to Ochanomizu University (through the Collaborative Organization for Research in women's Education of Science, Technology, Engineering, and Mathematics (CORE of STEM), Ochanomizu University).

References

[1] M. Kaminaga, "Introduction to Modern Cryptography," Kodansha B-2035, 2017.

[2] W. Diffie and M. E. Hellman, "New Directions in Cryptography," ***IEEE Transactions on Information Theory,*** IT-22(6), pp.64-654, 1976.

[3] R. L. Rivest, A. Shamir, L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," MIT-LCSTM-082, 1977.

[4] Internet Engineering Task Force (IETF), "The Transport Layer Security (TLS) Protocol Version 1.3," RFC8446, https://tools.ietf.org/html/rfc8446, 2018.

[5] K. Yamaguchi, A. Kuwana, K. Kagami, "Development of Teaching Materials for Cryptography at Senior High School", International Conference on Technology and Social Science 2020 (ICTSS 2020), IPS-02-b, 2020.

[6] The Ministry of Education, Culture, Sports, Science and Technology (MEXT), "High school subject area of Information (common subject area)," https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1416746.htm, 2020.

[7] V. Miller, "Use of elliptic curves in cryptography," ***Advances in Cryptology – CRYPTO '85,*** LNCS 218, pp.417-426, 1985.

[8] N. Koblitz, "Elliptic curve cryptosystems," ***Mathematics of Computation*** 48(177), pp.203-209, 1987.

[9] KH Coder, a software for quantitative content analysis or text mining: https://khcoder.net/en/