Journal of Technology and Social Science (JTSS)

Development of Hands-on Teaching Materials for Cryptography in 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. Cryptography is an essential technology used to secure current Internet communications. It is implemented against the background of the theory of difficulty in mathematics (e.g., the difficulty of prime factorizing large composite numbers). Additionally, cryptography is an ideal teaching material for learning mathematics and information technology. Since textbooks do not fully cover the theoretical aspects of cryptography, it is crucial to develop this technology. Therefore, this project aims to broaden the student base and develop teaching materials that interest children and students of various ages in mathematics and information technology. We developed graphical learning materials that can be used in class or at home for students to learn about cryptography. We believe that it will be beneficial for students and teachers to create more user-friendly and easy-to-learn learning materials based on the results of the previous year's materials.

1. Introduction

Cryptography is an important technology used to secure Internet communications. It is implemented against the background of the mathematical theory (e.g., the difficulty of prime factorization). Cryptography is an ideal teaching material for learning mathematics and information technology. It is essential to develop these technologies since textbooks do not fully cover their theoretical aspects. Thus, this project aims to develop teaching materials that interest children and students of different ages in mathematics and information technology.

In the 2022 school year, high school students will start learning new subjects based on new courses of study [1]. In the subject "Information," two new courses, "Information I" and "Information II," will be established, requiring students to learn more about science and mathematics.

According to the teaching materials for training teachers of "Information I" in high school [2], the subject covers "Information Security" in "Mechanism and Role of Information and Communication Networks" in "Chapter 4: Information and Communication Networks and Data Utilization." Although the terms of the authentication method, encryption method, and encryption algorithm are mentioned, the content of the encryption algorithm is not explained. Therefore, we would like to develop this educational program to reinforce and develop the contents of this part.

We developed a prototype of teaching materials in MS-Excel that allowed students to learn how to create ciphers last year [3]. We ported them to Scratch [4] so that they can easily run in a web browser. This year, we also developed a teaching material that challenges students to decipher ciphers. We aimed to make students understand the safety and danger of cryptography.

2. Developed Teaching Materials to Learn Caesar Cipher

2.1 How the Cryptography Works

The Caesar cipher used by Julius Caesar in ancient Rome is considered the beginning of common key cryptography [5]. 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 and decryption can be expressed by Eqs. (1) and (2), respectively.

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

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

2.2 Worksheet-Type Materials

Figure 1 shows the worksheet-type materials. They were written in Japanese; however, we translated them into English. The red text shows an example of students' entries. The worksheet also contains a conversion table for the Caesar cipher, with only keys 1–10 and only English capital letters as letter types in this worksheet. Students attempt encryption and decryption through the following steps:

- STEP 1: Students choose a common word from the dictionary and make it their plain text. For example, "FIRE."
- STEP 2: Choose one key and encrypt their plain text, which is chosen in STEP1 according to the conversion table. If a key is 2, "FIRE" becomes "HKTG."
- STEP 3: Exchange the ciphertext created in STEP2 with a pair (e.g., a classmate sitting next to them). The example student gave "ILUH" to the pair and received "DSSOH."
- STEP 4: Attempt to fix the "DSSOH" given by the pair into plain text. The example student tried 1, 2 as a key, in that order, and succeeded in deciphering the cipher by getting the plaintext "APPLE" with 3 as a key.

Through the experience of cryptanalysis, students can understand that the Caesar cipher is weak. In STEP 5, It considers the reasons and countermeasures. Here, the cipher can be deciphered in ten attempts. This is called a brute force attack. If the conversion table includes English uppercase and lowercase letters, numbers, and symbols, it will take longer to crack the cipher. Additionally, if the order of the characters is not "ABC" but random, it will be more difficult to decipher. However, if the eavesdroppers can steal the conversion table and key, they can easily obtain the plaintext. From this, students can also learn the disadvantages of common key cryptography.

2.3 Online Type Materials

We have also created teaching materials that can be run on a web browser so that students can study by themselves at home. It is shown in Fig. 2.

Clicking on the "Eavesdrop on ciphertext" button will randomly display the string from the worksheet STEP 2. If the students enter a number in the "Key" field, the deciphered plaintext will be displayed. As with the worksheet, they can decrypt the text by entering the keys from 1 to 10 in order. In this example, the ciphertext "DOZDBV" was decrypted, and the plaintext "ALWAYS" was obtained using key 3.

Caesar Cipher Conversion Table

KEY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

STEP1. Decide on one of your words, up to 5 letters.

F I R E

STEP2. Convert the words using the conversion table, and write down the KEY.

H K T G KEY 2

STEP3. Exchange the ciphertext in STEP 2 with your pair.

D S S O H ←Write down the ciphertext of your pair.

STEP4. Try to decipher the ciphertext of your pair.

C R R N G KEY:1

B Q Q M F KEY:2

A P P L E KEY:3

STEP5. This encryption algorithm is weak.

Let's try to figure out why and how to make it stronger.

Fig. 1. Worksheet-type materials for learning Caesar cipher. The red text shows an example of students' entries.

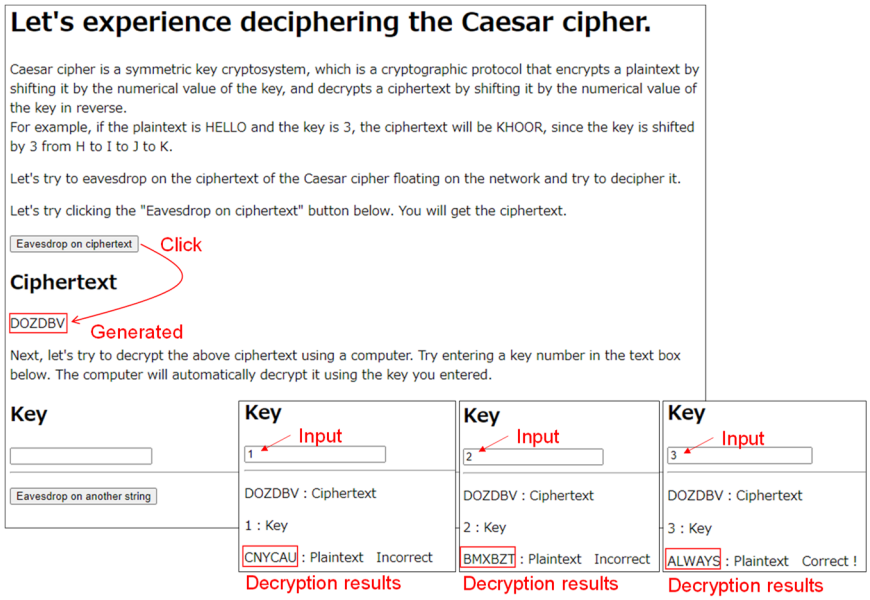


Fig. 2. Online type materials for learning Caesar cipher.

3. Materials for Learning Advanced Cryptography

The students understood that the Caesar cipher could easily be deciphered using the materials explained in Section 2. The next step for students is to learn advanced ciphers that overcome the disadvantage of the Caesar cipher. One of the disadvantages of Caesar cryptography is that it is a "common key cryptography." It means that the key must be sent securely to the cryptographic recipient. The solution to this problem is "public-key cryptography." The underlying method of public-key cryptography was introduced by Diffie and Hellman [6]. Additionally, RSA cryptography, one of the public-key cryptography methods, was created by Rivest, et al. [7]. A public key is used for encryption in public-key cryptography, and a private key is used for decryption. The security of RSA cryptography depends on the difficulty of prime factorization. It is a mathematical theory that guarantees the security of cryptography. The common key cryptography and the public-key cryptography can also be used in combination. In that case, it is called hybrid cryptography. For example, encrypted communication used in Internet shopping is called secure sockets layer/transport layer security (SSL/TLS) [8]. SSL/TLS uses a hybrid cryptography method.

We created teaching materials in MS-Excel to experience encryption procedures of the single-transform cipher [3]. This time, we ported the teaching material on RSA cryptography to Scratch [4] so that it can be run in a web browser (Fig. 3). We did not create a teaching material to challenge cryptanalysis because advanced cryptography, such as RSA cryptography, takes a long time to decipher. We only explained why it takes time to decipher them.

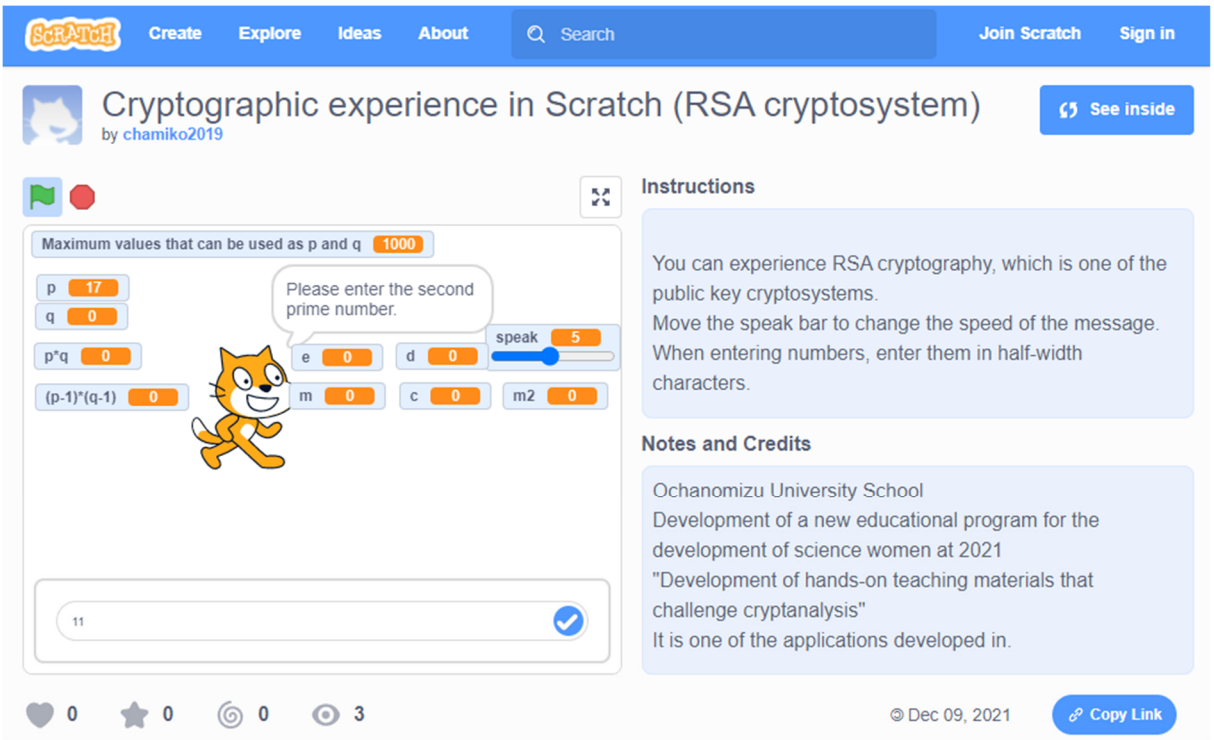


Fig. 3. Online type materials for learning RSA cipher

4. Practice in High School Class

One hundred and twenty first-year high school students in Japan (about 40 students, 3 classes, Ochanomizu University Senior High School) participated in a cryptography class using teaching materials explained in Sections 2 and 3. Figure 4 shows that the teacher explained the mechanism and principle of cryptography using a blackboard and slideshows.

Figure 5 shows the results of the questionnaire survey conducted after the class, comparing the results for FY2020 [3] and FY2021. According to the result of Fig. 5 (f), there are more students who

do not know about cryptography than in FY2020. Nevertheless, Figs. 5 (a), (b), and (c) show that the number of students who answered that the class improved their motivation to learn is more than FY2020. The newly developed teaching materials can improve the interest of beginning learners. However, the number of respondents who lost interest in learning increased from Fig. 5 (c). They answered that the class was difficult and fast. The number of students who answered "very difficult" and "very fast" increased in Figs. 5 (d) and (e); therefore, it is necessary to examine the progress and content of the class more carefully.

There are two possible reasons for the increase in the number of students who are not familiar with cryptography: first, as the Internet has become more familiar, more students do not bother to learn about cryptography. Second, in the limited class time, there are more opportunities to learn about data science and AI, and fewer opportunities to learn about cryptography. If they are correct, we think the trend of more students not familiar with cryptography will continue. However, if movies based on cryptography become popular, such as "Summer Wars" in 2009, many students will be very interested in cryptography and will study it themselves.

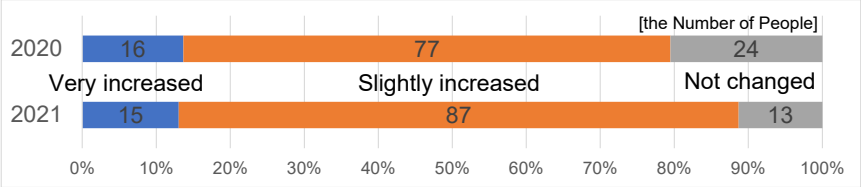
Fig. 4. Photos of the class

5. Conclusion

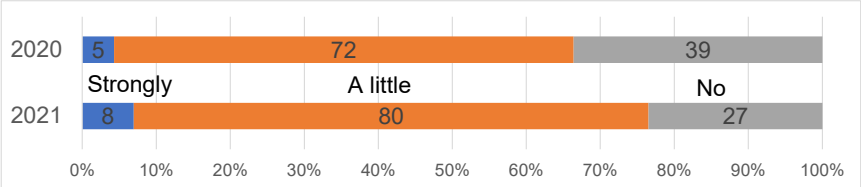
We have developed teaching materials for learning cryptography and used them in a class for first-year high school students. We improved the interest of students who did not know about cryptography compared to FY2020. However, we need to consider the difficulty and progress of the class. We aim to develop teaching materials that can easily be used by teachers who are not specialists in information technology. We will publish the teaching materials and study plan on our website [9]. This paper deals with Caesar cipher and RSA cryptography as examples, because these are widely known. As of FY2021, we have released Caesar, RSA, and Vernam cipher as web applications (only Caesar and RSA are available in English). In FY2020, in addition to Caesar, RSA, and Vernam, we created a prototype of simple substitution cipher and Diffie–Hellman key exchange in MS Excel. We would like to publish also these ciphers as web applications in the future.

Acknowledgments

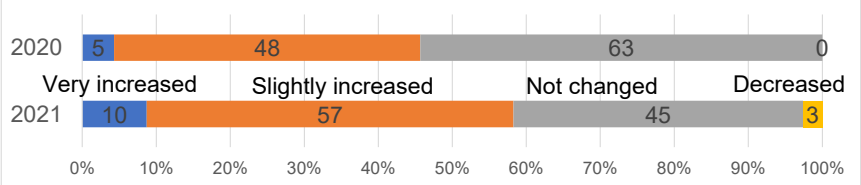
We gratefully acknowledge the support of the new educational program development project for educating women in science at the schools attached to Ochanomizu University (through the Collaborative Organization for Research in women's Education of Science, Technology, Engineering, and Mathematics (CORE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



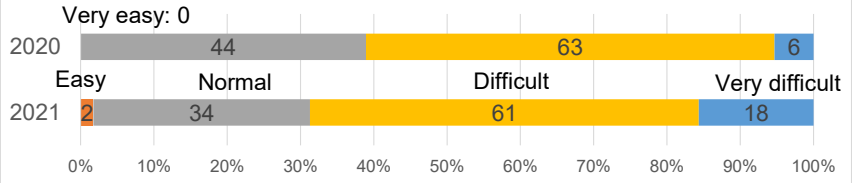
(a) After taking this class, did your interest in encryption increase?



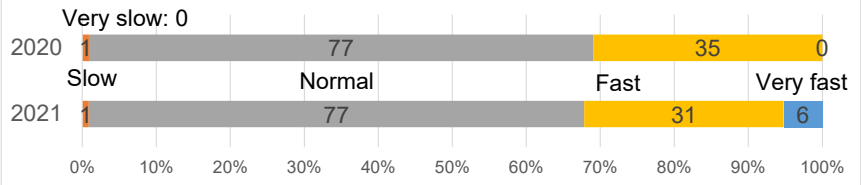
(b) After taking this class, do you want advanced learning?



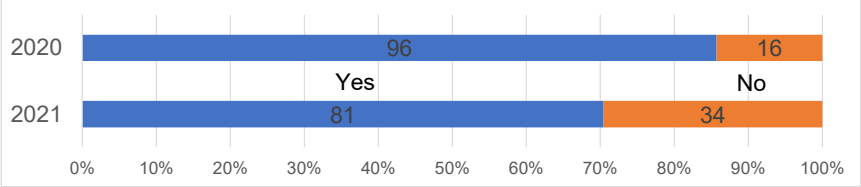
(c) After taking this class, did you feel more motivated to study the encryption?



(d) Difficulty level of the class



(e) Progress speed of class



(f) Have you known that cryptography is used in Internet communications before taking this class?

Fig. 5. Results of the questionnaire survey conducted after the class, (Number of respondents: FY2020: N = 116, FY2021: N = 115), (Some respondents did not fill in some parts of the questionnaire in FY2020)

References

[1] The Ministry of Education, Culture, Sports, Science and Technology (MEXT), "New learning guidance": https://www.mext.go.jp/a_menu/shotou/new-cs/index.htm

[2] 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

[3] K. Yamaguchi, A. Kuwana and K. Kagami, "Development of Teaching Materials for Cryptography at Senior High School," ***Journal of Technology and Social Science***, Vol.5, No.1, pp.41-46, 2021.

[4] Scratch: https://scratch.mit.edu/

[5] M. Kaminaga, "Introduction to Modern Cryptography," Gendai Angou Nyumon (in Japanese), Kodansha B-2035, 2017.

[6] W. Diffie and M. E. Hellman, "New Directions in Cryptography," ***IEEE Transactions on Information Theory***, Vol.22, No.6, pp.64-654, 1976.

[7] R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," ***Communications of the ACM***, Vol.26, No.1, pp.96-99, 1977.

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

[9] Ocha Algo: https://ocha-algo.com/