CRYPTOGRAPHY FOR MIDDLE SCHOOL STUDENTS IN AN EXTRACURRICULAR LEARNING PLACE

Nadine Bergner, Jan Holz and Ulrik Schroeder
Computer-Supported Learning Research Group, RWTH Aachen, Ahornstr. 55, Aachen, Germany

Keywords: Extracurricular Learning Place, Course Design, Learning Methodologies, Blended Learning, Collaborative Learning.

Abstract: In order to inspire middle school students for computer science topics we developed a two-day-course about cryptography. Thereby we try to counteract the relatively low interest in STEM (science, technology, engineering and mathematics) topics by offering engaging insights into computer science. This course is one of several workshops within our extracurricular learning place for computer science called InfoSphere. The fundamental idea of the presented workshop is to provide a first insight into the world of cryptography for middle school students. During the course groups of three to five students discover the four different cryptographic methods Skytale, Fleißner Template, Caesar Encryption and Vigenère Encryption on their own. We designed the course according to the didactic principle of exploratory learning, so the participants can learn action-oriented and at their individual learning rate. In conclusion we discuss the results of a first evaluation with a test group of 23 students (17 girls and six boys).

1 INTRODUCTION

Now and in the future Germany, like many other countries, has the problem of having too few well educated computer scientists. One reason for this is the low interest in STEM (science, technology, engineering and mathematics) among school students. We try to counteract this by offering engaging insights into computer science for school students. The presented course is one of several workshops within our extracurricular learning place for computer science called InfoSphere. These courses are developed to motivate children to get in contact with computer science topics.

We chose the topic cryptography, because it is not included in regular school lessons, but is suitable to show that computer science has to offer much more than just programming. This is part of our overall goal to convey an idea about computer science which is as realistic as possible. Furthermore we particularly aim at addressing girls and students who are generally less interested or less promoted in STEM topics, as can be seen within our project IGaDtools4MINT. We try to motivate especially these target groups by discussing security aspects with a strong link to the students' everyday lives (e.g. login on websites like Facebook).

The cryptography workshop is designed as a two-day-workshop for twelve to twenty participants at the age of eleven to fourteen. The course itself can be visited by heterogeneous groups with students of different ages, so that they can benefit from each other because of their different prior knowledge.

The participants work in four parallel groups of three to five students and they develop the different tasks and puzzles step-by-step on their own. We created various hands-on learning materials to address as many senses as possible and manage the whole course without classical worksheets. Our inspiration comes from Janette Griffin: "[...] important features of programs which engender long-term learning and interest are: planning; consideration of the unique learning opportunities of the institution rather than mirroring school-type use; variation in the activities during the visit; sparing use of worksheets; and emphasis on first-hand experience and observation." (Griffin, 1994, S. 121)

Within this concept the students are able to learn at their own speed, which is a very important didactical advantage (see Aepkers et al., 2002). To support an individual learning rate, a specifically developed software program leads the students through the course step by step. To continue within

Bergner N., Holz J. and Schroeder U..
CRYPTOGRAPHY FOR MIDDLE SCHOOL STUDENTS IN AN EXTRACURRICULAR LEARNING PLACE.
DOI: 10.5220/0003920002650270
In *Proceedings of the 4th International Conference on Computer Supported Education* (CSEDU-2012), pages 265-270
ISBN: 978-989-8565-07-5

the program the students have to understand each cryptographic method and give correct answers to corresponding questions. Therefore it is unnecessary to control the students at any time.

We will start with explaining the idea of the extracurricular learning place for computer science called InfoSphere. After this we give an overview about the cryptography course with our motivation, the main idea and the structure of the two-day-workshop. Section 3 describes the workshop in detail and gives an insight in the used learning materials. Afterwards we summarize the results of the first test run with a group of 23 middle school students. Thereby we report our impressions and the feedback of the participants, resulting in an outlook on our future work. Closing up Section 6 gives a final summary.

2 INFOSPHERE - AN EXTRACURRICULAR LEARNING PLACE FOR STUDENTS OF ALL AGES

An extracurricular learning place serves to teach specific topics of one field to students of different ages. The InfoSphere is an extracurricular learning place especially for computer science topics. It opened in summer 2010 under the leadership of the Computer-Supported Learning Research Group of the RWTH Aachen University (see Lehr- und Forschungsgebiet Informatik 9). The InfoSphere offers several perspectives on numerous facets and applications of computer science for students of all ages and types of school beginning with class three.

The InfoSphere provides courses as an addition to regular school lessons. In Germany, North Rhine-Westphalia there are no obligatory computer science lessons in school. This is the reason why many students do not get in contact with computer science topics during K-12. This in turn leads to the problem of many first-year students in computer science having a wrong idea about computer science studies (Heine, 2006); (Maass und Wiesner, 2006). High dropout rates during the first semesters at university are the result (Heublein et al., 2010). Besides correcting the students' idea of computer science and encouraging interest in this field we try to reduce these dropout rates by providing a publically available extracurricular learning place.

For achieving this, the InfoSphere offers a wide range of courses for half a day, a full day, or several days. These courses provide experimental and action-oriented learning with a link to the students' everyday experiences. One of the essential features of InfoSphere courses is the very individual access they offer for the different topics. Combined with self-directed learning and peer-teaching, this should encourage school students to discover the various aspects of computer science on their own. Our idea is to enable a learning process that is as natural, exciting and self-discovering as possible. By this these courses should help to raise interest in computer science even for those who are not tech-savvy or did not get in contact with computer science so far. Another motivation to open an extracurricular place of learning was to assist computer science teachers and students in teacher training in teaching novel topics and becoming more familiar with modern learning materials, methods and media. InfoSphere has been designed as a research laboratory to test and practice different learning experiences. Moreover, it offers a plethora of modern media and technology (e.g. multi touch tables, smartphones and interactive whiteboards) to help trainee teachers implement innovative learning scenarios. Furthermore, students in teacher training get the chance to acquire crucial media competences in practice. For these reasons the courses are designed by two to four students in teacher training under supervision of the members of the teacher training chair.

Within the InfoSphere we investigate the following research questions.

- How can an extracurricular learning place like InfoSphere help to convey a realistic picture of computer science?
- What are the most significant criteria to change the existing stereotypes about computer science?
- How can we correct the picture for different target groups?
- What should a workshop look like to create this picture as realistic as possible?
- What are the crucial differences between male and female participants?

3 PROCEDURE OF THE CRYPTOGRAPHY COURSE

At the beginning of the first day we start with a get-to-know-round, because the students know neither each other nor us. After this we randomly split the participants into four groups. To increase motivation we show each student group a treasure chest which is locked and send them on a hunt for the right key.

Afterwards each group gets a laptop and starts the accompanying program. In the first step they can choose one of four avatars, which lead them through the program and a name for their group (see Figure 1: Screenshot of the intro screen).

Figure 1: Screenshot of the intro screen.

After this, Skytale is introduced as the first cryptographic method (Hebisch 2010); (Kaul, 2006). It is a very easy method, which was used by the Spartans around fifth century BC. To encrypt a text you have to wrap a small paper strip around a wooden stick (see Figure 2: Skytale), write the text horizontally on the paper strip and loose it from the stick.

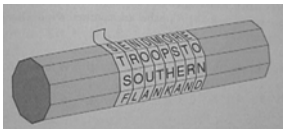


Figure 2: Skytale.

After this a foreign person cannot read the text because the letters are disordered. To decode the text the receiver has to know which diameter the stick must have. Otherwise s/he has to try all possible diameters of the stick until s/he can read the message.

Instead of explaining the method to the students we provide some wooden sticks and labelled paper strips and let the students guess how this technique works. The program requests two words from the encrypted text to see if the group has decoded it right. The supervisors keep themselves in the background unless the students ask especially for help. In these cases the supervisors give little hints to help the students to find a solution on their own. For detailed information about the didactical method “discovery learning” see Aepkers (Aepkers et al., 2002).

After every student has understood the way to decode a text with the Skytale method, they have to encode another text. Only when the group can en- and decode a text with the Skytale method, the program allows them to get to the next section.

The second cryptographic method the students get to know is the *Fleißner Template* (see Brätz, 2010). This method exists since 1881 and needs only a square paper template (see Figure 3: Fleißner template). A specific restriction of this method is that the text has to consist of 4, 16, 36 or 64 etc. letters because of the 2x2, 4x4, 6x6 or 8x8 square. In the following we use a 36 letter example. To encode a text you have to write the first nine letters into the gaps of the template from top to bottom and from left to right. After that you have to rotate the template clockwise by 90° and go on with the next nine letters. Finally you have a square of 36 letters which seems to be arranged in a random manner. To decode such a square of letters the receiver has to know how the Fleißner template has to look like, that means where the gaps are. Otherwise s/he has to try all possibilities for a 6x6 square with 9 gaps.

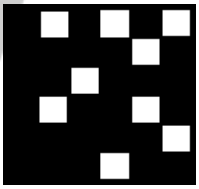


Figure 3: Fleißner template.

Similar to our procedure with the Skytale method we give a Fleißner template and a paper with a square of 36 letters to every group of students. The program again requests the students to guess how this method works. When they use the given template in the right way they can read a simple question. After entering the correct answer into the program, it shows the students a new message, which then should be encoded with the Fleißner template. Only if the groups enter the decrypted message in the program (see Figure 4: Screenshot of the section Fleißner template) and shows that they understand the de- and encryption with the Fleißner template the program allows them to discover the third cryptography method.

As a third method the students get in contact with the *Caesar Encryption* (Freiermuth, 2010). This method works with a shift of all letters by a defined code letter in the alphabet. For example if you shift every letter by the code letter “D”, you have to replace an “A” by a “D”, a “B” by an “E” etc. To simplify this process you can use a disk with two

alphabets on it, so that you only have to rotate it to the right position (see Figure 3: Caesar disc). After this you can replace every original letter by the one next to it on the disc. If the receiver does not know the right code letter s/he has to try all 26 different possibilities.

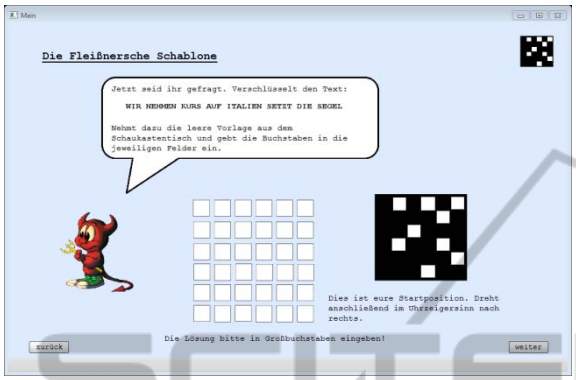


Figure 4: Screenshot of the section Fleißner template.

Figure 5: Caesar disc.

Like the two times before the groups get the learning material and can check out the different options on their own. In this case they get a text where the first letters are already decrypted to give them a hint how they have to turn the Caesar disc. After the students have found out the right code letter, they can decrypt the whole text without any problems. The second step is to encrypt an answer message to send it back. When the students solve this task as well the program leads them to the last cryptographic method.

The last introduced cryptographic method is the *Vigenère encryption* (Freiermuth, 2010). This method is an extension of the Caesar method, where every letter is encrypted by a different Caesar shift. That is the reason why you need not only one code letter, which determines the shift, but a code word (here for example "KEY") so that each letter defines a different shift. If you want to encrypt the letter "D" as the first letter of your text, you have to use the first letter of your code word "K" and therefore replace the "D" by a "N" (see Figure 6: Screenshot of the section Vigenère encryption).

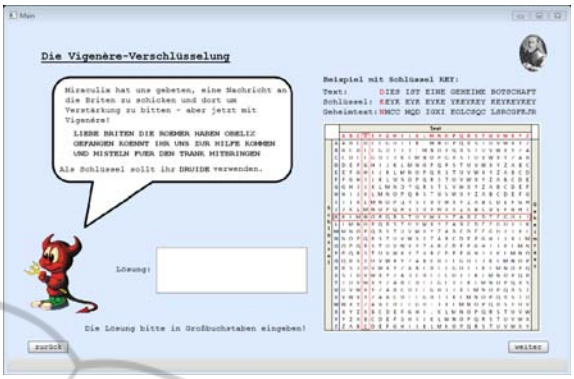


Figure 6: Screenshot of the section Vigenère encryption.

When all four groups have finished the program, each group gets the task to prepare a short presentation about one of the four cryptographic methods including its advantages and disadvantages. In the following discussion round we talk about how save each method is respectively how much effort is necessary to crack the method. It is important not only to know how the methods work but also for which texts they are useful. Therefore they can take pictures with digital cameras of themselves and the material or produce short video films to explain the different methods. The students are encouraged to design a creative presentation, which they present to the other participants, the supervisors and their families. Furthermore we look out on computer assisted methods, which can be developed in an advanced workshop.

At the end of the workshop the students are able to open the treasure chests from the beginning and unpack the sweets, which is a great reward for them.

4 RESULTS AND FEEDBACK

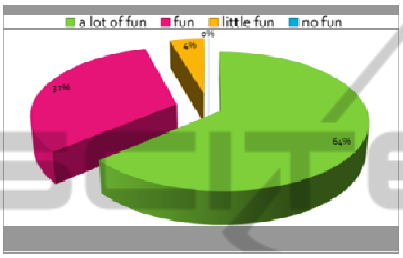
First of all the list of participants with 23 students (17 girls and 6 boys) on it shows that the topic cryptography is popular among twelve to fifteen year old students (the aimed maximal number of participants was 20). It seems to be especially interesting for girls. The rate of female to male students (female: 73.9 % to male: 26.1%) is extraordinary for a computer science workshop. Mostly there are much more boys than girls in the groups visiting us (34.1 % girls on average in 2011).

The overall outcome of our test run is that the students' learning rate is higher than expected. The

participants completed the whole course in about 6 hours.

The course itself shows that it is very worthwhile to design workshops with a lot of teamwork. It is really remarkable how much the students learn from each other and how little help of the supervisors is needed. Also the students report back that it is (a lot of) fun to work in groups (see Diagram 1: Percentage values to: "It was fun to work in groups.").

Diagram 1: Percentage values to: "It was fun to work in groups."



Some of them say that it would be greater to choose the groups on their own, but we intentionally mix the groups so that everybody has the chance to get to know new people. Otherwise it is very difficult for single participants to get into contact with an existing group. Besides this remark all participant enjoyed it to work in groups.

As expected the four groups do not work at the same speed because of the different ages and prior knowledge. This fact was calculated in advance. So we integrated special tasks and encourage the students to help each other.

Additionally the evaluation shows that the course motivates the majority of participants to follow up other topics of computer science because they experienced that computer science is really interesting. Some students were very surprised that computer science includes topics like cryptography as well. To evaluate what students associate with the term computer science we ask the students before and after the course which three words they associate with computer science. In both surveys the most frequently mentioned answer was “computer”, but in opposite to “programming”, “mathematics”, “studies” and a list of programming languages before the course, after the course some students answer “cryptography”, “puzzles”, “problem solving” and even “fun”. For detailed data see Diagram 2: keywords before the course and Diagram 3: keywords after the course.

Diagram 2: Keywords before the course.

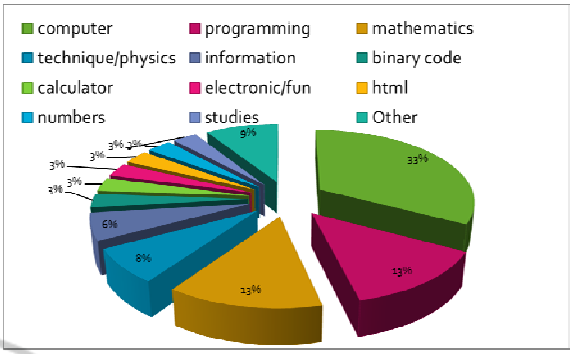


Diagram 3: Keywords after the course.

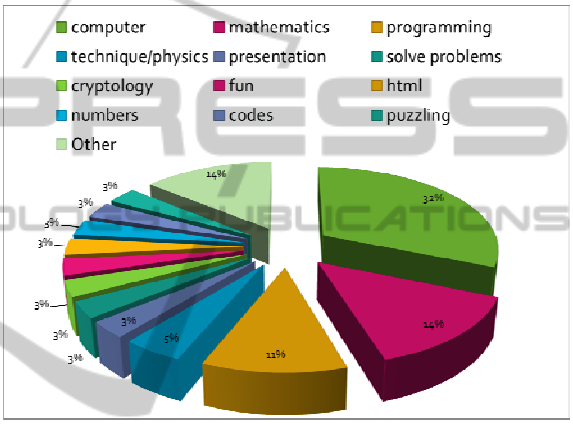
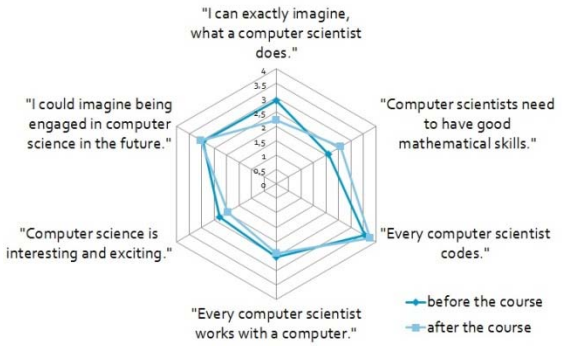


Diagram 4: Students’ ideas of computer science.



Furthermore we analyzed the student’s idea of “computer science” in general. To figure out if the cryptography course is able to change this idea a bit, we consult the students before and after the course. Diagram 4: students’ ideas of computer science contrasts the results. This shows that the cryptography course is able to change the students’ idea of computer science a little bit in short time, but there is no evidence for a long lasting change. Our assumption regarding long term changes is that it is

helpful and necessary to offer multiple courses over a longer time.

5 FUTURE WORK

On the basis of the test run we plan to expand the course with a fifth cryptography method (Enigma decryption). We are going to convey the history and functionality of the Enigma. This would be an additional part, which can be used flexible depending on the learning group. Furthermore we are going to develop an advanced cryptography workshop about computer assisted methods.

Based on the limited space in front of the laptops, we are going to reproduce all materials to enable a group size of three.

Furthermore we aim to publish the materials on our website, so that middle school teacher can use it for their courses in school if they do not have the possibility to visit the InfoSphere. However this would mean a lot of preparatory work to build all the hands-on materials.

In order to reach additional target groups we are going to develop equivalent courses for other classes with different computer science topics. Currently we are working on courses for computer graphics in class twelve and logical circuits in class eight.

6 CONCLUSIONS

Altogether the cryptography course is a great way to reach out to those students, who are not yet excited by computer science. Especially for girls teamwork is very important. Apart from that female and male students enjoy it to be creative in designing presentations and like it to present their own work. It is essential to present computer science to middle school students in an interesting and exciting way, because this is the time of life where most of them, especially girls loose the interest in STEM topics.

Above all we are going to add this course to the regular offering at our extracurricular learning place for computer science topics InfoSphere.

REFERENCES

Aepkers, Michael, Liebig, Sabine, Bönsch, Manfred, and Kaiser, Astrid. *Entdeckendes, forschendes und genetisches Lernen*. Baltmannsweiler: Schneider-Verl. Hohengehren, 2002.

Brätz, Marcel. “Kryptographiespielplatz.” 2010. http://www.kryptographiespielplatz.de/, accessed November 2011.

Freiermuth, Karin, ed. *Einführung in die Kryptologie: Lehrbuch für Unterricht und Selbststudium.* 1st ed. Wiesbaden: Vieweg + Teubner, 2010.

Griffin, Janette. “Learning to learn in informal science settings.” *Research in Science Education* 24, no. 24 (1994): 121–128. http://www.springerlink.com/content/655l35n85236455u/fulltext.pdf, accessed October 2011.

Hebisch, Udo. “Skytale.” 2010. http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/skytale.html, accessed November 2011.

Heine, Christoph. *Ingenieur- und Naturwissenschaften: Traumfach oder Albtraum?: eine empirische Analyse der Studienfachwahl*. Baden-Baden: Nomos, 2006.

Heublein, Ulrich, Hutzsch, Christopher, Schreiber, Jochen, Sommer, Dieter, and Besuch, Georg. “Ursachen des Studienabbruchs in Bachelor- und in herkömmlichen Studiengängen.“ 2010, accessed December 2011.

Kaul, Daniel. “Skytale, Caesar & Co. - Verschlüsselung in Antike und Mittelalter.” 2006. http://www.phil.uni-passau.de/histhw/TutKrypto/tutorien/verschluesselung-antike-mittelalter.htm, accessed November 2011.

Lehr-und Forschungsgebiet Informatik 9, RWTH A. “Schülerlabor Informatik - InfoSphere.” http://schuelerlabor.informatik.rwth-aachen.de/, accessed December 2011.

Maass, Susanne, and Wiesner, Heike. “Programmieren, Mathe und ein bisschen Hardware … Wen lockt dies Bild der Informatik?” *Informatik-Spektrum* 29, no. 2 (2006): 125–132.