A Short Introduction to Classical Cryptology as a Way to Motivate High School Students for Informatics

Lucia Keller, Barbara Scheuner, Giovanni Serafini, and Björn Steffen

Department of Computer Science, ETH Zurich, Switzerland
{lucia.keller,barbara.scheuner,giovanni.serafini,
bjoern.steffen}@inf.ethz.ch

Abstract. In Swiss high schools, programming is the typical content of an introductory informatics course. This is an important topic, but nevertheless it is only a part of the field. By integrating short introductions to other topics, students get a better understanding of the broadness of informatics.

This article presents such a short introduction unit about classical cryptology without requiring any school-related prior knowledge in informatics. The basis of this unit is the everlasting game between code designers and code breakers to build, respectively break, cryptosystems. The challenge of breaking the codes presented by the teacher is the core and motivating factor of our didactical concept. Although the theoretical concepts cannot be presented in detail, the unit demands analytical skills and encourages critical thinking.

The unit motivated 70 % of the participating students to learn more about the topic, which is a good pre-condition for subsequent cryptology courses.

1 Introduction

Cryptology is nowadays an interdisciplinary research field, which integrates elements of mathematics [1,3], algorithmic fundamentals of computer science [8] as well as physics [4]. Moreover, cryptology is an exciting school subject, which allows the combination of the student's real-life experiences with deep scientific knowledge. Students of different ages and with different abstraction skills can be introduced to the basic mechanisms of cryptology.

Koblitz stated already in 1997 the impressive value of cryptography as a teaching tool. In his article [12] he highlighted his didactic approach and his experiences teaching symmetric and public-key cryptography concepts to children of primary schools. Bell et. al. devoted some of their off-line activities and games to cryptology in *Computer Science Unplugged* [2]. Also the very popular book of Singh [13] shows that the history behind cryptology can attract a large audience.

Our paper relies on a similar didactic concept, but describes a teaching sequence especially for high school students, which only focuses on classical cryptography and, therefore, handles more cryptosystems than Koblitz did. This

I. Kalaš and R.T. Mittermeir (Eds.): ISSEP 2011, LNCS 7013, pp. 189–200, 2011.

teaching unit does not require any school-related prior knowledge in informatics. It is designed as an interaction between the code designer (the teacher) and the code breakers (the students). While the mere encryption of a given plaintext and the decryption of an available cryptotext soon becomes annoying, students challenged to break cryptosystems are really involved and implicitly adopt a critical attitude regarding scientific subjects.

The introduced teaching unit on classical cryptology is a part of a comprehensive collection of teaching materials for high schools developed at ETH Zurich during the last five years. The authors attach importance to a precise and understandable explanation of concepts and notions. This is an important basis for a profound comprehension of the design and the analyis of the introduced cryptosystems. Those books are self-contained and can be used for individual learning [5]. The basis of the presented teaching unit are chapters 1 to 3 (90 pages) of the textbook about cryptology. The whole book is covering topics such as classical and modern cryptology, symmetric and public-key cryptosystems, zero-knowledge protocols as well as their mathematical and algorithmic fundamentals [6]. This teaching unit was intensively tested in some informatics classes and during several project weeks or single visits aiming to promote informatics at high schools. For a thorough discussion of those chapters we allocate 18 lessons in a informatics class in the last year of high school.

The goal of our teaching unit is not a thorough discussion of this topic but to give the students some interesting insights to classical cryptology without using the formal language of mathematics too intensively. We want to elate the students for informatics and to motivate them for visiting further informatics courses. Therefore, we use classical cryptosystems, although they are far from satisfying modern security requirements. But they represent an essential didactic tool in order to introduce the basic concepts and the well-established, precise terminology of cryptology.

The paper is organized as follows: in Section 2, we introduce the concepts of classical cryptology as well as the basic terminology. After that, we describe the main idea, the goals and the structure of the teaching unit. Section 3 presents a sample lesson held at the beginning of 2011 at the high school MNG in Zurich and discusses the results of a survey the students had to complete in conjunction with the sample lesson. We conclude with general reflections on our experiences dealing with motivation, expectations and achievements introducing high school students to classical cryptology in Section 4.

2 Classical Cryptosystems and the Concept of Security

It is important to determine the terminology before starting to introduce examples of cryptosystems.

We consider *classical cryptosystems* as symmetric (secret-key), paper-and-pencil cryptographic systems, which were conceived and employed in the pre-computer era.

A person, called the *sender*, wants to send a message (the *plaintext*) in a natural language to a second person, the *receiver*. The plaintext will be sent over

an insecure channel. Hence, the message may be eavesdropped by an unauthorized person. Therefore, we have to *encrypt* the message with a secret key such that we can send the *cryptotext* over the insecure channel. The receiver *decrypts* the message with a method that inverts the encryption. Such cryptosystems are called *symmetric cryptosystems* because the sender and the receiver encrypt and decrypt with the same secret key.

2.1 Security of Cryptosystems

It is naive to assume that it is adequate to keep the method of *encryption* and *decryption* secret between the sender and the receiver. In 1883, Kerckhoffs formulated the so called *Kerckhoffs' Principle of Security*:

> *A cryptosystem is secure, if one, knowing the art of the functioning of the cryptosystem but not knowing the key used, is not able to derive the original plaintext from the given cryptotext.* ([8], cf. [10,11])

Nowadays, being not able to derive the original plaintext means that the unauthorized person is not able to find the plaintext with his actual computational resources in reasonable time. In some applications, reasonable time means 10 seconds and in other applications it means 30 years. This depends on the importance of the plaintext and the time how long a cryptotext has to remain confidential. We will see that it is not sufficient for building secure cryptosystems to have a huge number of keys, but there also must not exist an efficient algorithm that can break a cryptotext without the knowledge of the key.

According to Kerckhoffs' Principle of Security, a secure cryptosystem has not to be kept a secret. Also if an enemy knows everything about the cryptosystem, he is not able to decrypt a cryptotext without knowing the key. Hence, the security only depends on the secrecy of the key and the strength of the cryptosystem.

In this paper, the plaintext is encrypted without punctuation marks and spaces. For example, the sentence

> This is a sample sentence.

is transformed to

> THISISASAMPLESENTENCE

before encrypting it.

3 The Didactical Concept of the Lecture

In the following, we describe how we introduce the students to classical cryptology. The presented lesson takes about 90 minutes and is only meant to give an overview of the topic. A thorough introduction would need much more time (approximately 18 lessons) as classical cryptology is strongly related to non-trivial concepts of probability theory and algorithmics which are used for the design

and the analysis of the cryptosystems. A detailed descryption of a longer introduction of classical cryptology can be found in the textbook [6]. A shorter introduction is given by Hromkovič [8,7]. Nevertheless, we focus on clear explanations of concepts and notions as a basis for following lessons.

3.1 Teaching Goals

The principal aim of our teaching unit consists in influencing the attitude and the interest of high school students with respect to cryptology and its applications in real-life: we expect that after completing the teaching unit, the students are aware of the relevance of cryptology for today's life and in particular for secure communication systems. At the same time, we try to stimulate the student's interest on cryptology and informatics in general and possibly to motivate them to learn more about this topic.

Students attending the teaching unit presented in this paper acquire concrete, observable skills and capabilities: they know and understand the concepts of cryptosystems, sender, receiver, eavesdropper, encryption, decryption, secret-key, plaintext, cryptotext as well as the definition of the concept of security for cryptosystems. Students correctly explain all these concepts to school colleagues without prior knowledge in cryptology, in a non-formal way, relying on the introduced terminology and the presented graphical schemes.

Students are able to correctly deal with the presented classical cryptosystems and to encrypt and decrypt simple messages by hand (without a computer). Given a message encrypted with one of the presented cryptosystems, students are able to compute the size of the key-space and to break the encryption carrying out a cryptotext-only-attack, by hand, working alone or in small groups.

3.2 Introducing the Concepts of Cryptology

In the following, we summarize our teaching unit divided in 9 steps.

Step 1: Introduction. We start with a short introduction where we briefly mention some applications of cryptology to motivate the students for these two lessons. Some of them are listed in [8].

Step 2: Two Ciphers. One of the first known ciphers[1] is POLYBIOS. The greek writer Polybios arranged the Greek alphabet, consisting of 24 characters, in a 5x5-matrix from left to right and top to bottom. To encrypt, he replaced every character by a pair, the number of the row and the number of the column.

Another well-known possibility to encode characters is the cipher FREEMASON. It was invented in the 18th century. Every character of the alphabet is replaced by the lines and dots in the neighbourhood of the character (see Fig. 1).

[1] Note, that we distinguish the words *cipher* and *cryptosystem*. Cryptosystems use keys for encryption and ciphers do not.

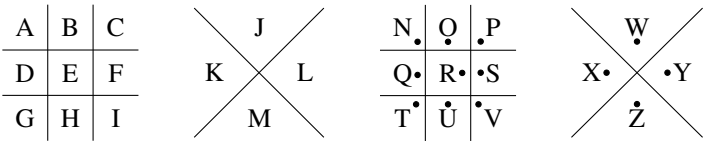
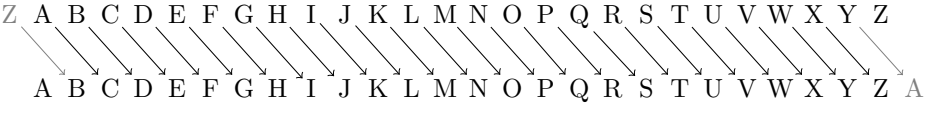


Fig. 1. The FREEMASON cipher [13]. Some examples: A = ⌟, J = ⋁, S = ⊏, Z = ⋀, and so on.

Step 3: Cryptosystems. At this point, we ask the students why the mentioned ciphers are not practicable and secure. The students immediately see that it is sufficient to know which cipher is used for the cryptotext and then it is easy to decrypt since you can consult the table. Therefore, we need more involved ciphers. Those ciphers should have the property that you do not have to keep the method of encryption secret but only the key. Hence, you need ciphers with a larger variety to encrypt. Those ciphers are called cryptosystems. The two ciphers from Step 2 are not cryptoystems because they do not have keys.

Step 4: The Cryptosystem CAESAR. The probably most popular cryptosystem is CAESAR. In this cryptosystem every character is shifted cyclically by a fixed amount of positions indicated by the key. In the following picture, the key is 2:



This cryptosystem has only 26 keys and hence, is easy to break for an unauthorized person. One can, for example, try exhaustively all keys and if a reasonable text shows up one can assume that the plaintext was found. However, it highly depends on the plaintext and the cryptosystem, if such a brute-force cryptanalysis can succeed in general or not.

Cryptology was and still is a game between the code designers and the code breakers. The **code designers** always try to invent new cryptosystems that are secure and the **code breakers** want to break those systems. We use this game to get the attention of the students. During the whole lecture, the teacher plays the role of the code designer and the students break the systems. This motivates the students because, finally, they can for once correct the teacher. Moreover, the kids also have fun solving puzzles.

Step 5: The Cryptosystem SKYTALE. To get a better cryptosystem, we have to design one with more keys. One possibility is the cryptosystem SKYTALE. The sender and the receiver have a wooden stick with the same diameter. The sender wraps a paper or a leather strip around the stick and writes the

message row by row onto the paper such that he places one character on one winding of the strip. The amount of characters on one winding (the diameter) is the key of the cryptosystem. If the strip is unwrapped, we get the cryptotext. The receiver has to again wrap the strip around the stick in order to read the plaintext. But how many keys do we have? It is easy to see, that this number depends on the length of the text, say n. In this case we have at most n possible keys. But not all keys make sense. In practice, the number of keys is not very large.

Afterwards, we shortly discuss one problem with the cryptosystem SKYTALE. The blanks at the end of the written message give the cryptanalyst a hint about the size of the key. How can we hide these blanks? Usually, the students have some ideas like filling in arbitrary characters at the end of the text, or adjusting the size of the key and the number of windings to the length of the text, such that there will not be any blanks at the end of the text.

Note, that this cryptosystem is based on a different principle than the previous one – instead of replacing symbols we change their positions.

Step 6: The Cryptosystem RICHELIEU. The last simple symmetric cryptosystem we want to introduce is RICHELIEU. This system was invented in the 17th century by the cardinal Richelieu. He used a cardboard where some holes are punched in. Then he writes the plaintext onto the paper through these holes. Afterwards he removes the cardboard and filles in the gaps with arbitrary characters to get the cryptotext. The receiver can decrypt the ciphertext by placing the same cardboard with the same holes on top of the cryptotext. How many keys do we have? Suppose that the number of rows on this cardboard is m and the number of columns is n. Each field on this cardboard can either be punched out or not. Hence, we have two possibilities for every field and $2^{m \cdot n}$ is therefore the total number of keys.

If the students are familiar with combinatorics, then they have no problems to figure out the number of keys. Otherwise, the teacher has to help the students, but also in classes with younger students, it was never a problem to explain how the number of keys is calculated.

Step 7: An Exercise. The Spartans want to send a secret message from Sparta to Athens. In this message, a strategy for the upcoming battle is described. The battle begins in 3 days.

The goal of the Spartans is to encrypt this message in such a way that the enemies need more than 3 days to break it. The Spartans know that the enemies have only one cryptanalyst. He is very smart and works efficiently. For one trial to decrypt the cryptotext, he needs only 1.5 minutes. This trial corresponds to testing one key. The unresting cryptanalyst can work three days and three nights at a stretch. The Spartans have to reckon that the smart cryptanalyst knows which cryptosystem is used for the encryption.

The Spartans decide to use the following cryptosystem:

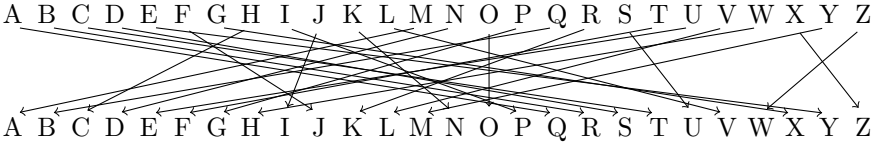
Cryptosystem 3DAYS

plaintext alphabet:	Latin characters
cryptotext alphabet:	Latin characters
set of keys:	(i, k, j) with $i, j \in \{0, 1, \ldots, 25\}$ and $k \in \{1, 2, \ldots, 100\}$
encryption:	Encryption in 3 steps: 1. Encrypt the plaintext with CAESAR and key i to $text_1$. 2. Encrypt $text_1$ with SKYTALE and key k to $text_2$. 3. Encrypt $text_2$ with CAESAR and key j to $text_3$.

Describe the decryption of a message encrypted with 3DAYS. Did the Spartans make a good choice?

Most of the students realize that SKYTALE and CAESAR are independent and that therefore the order of the encryption steps is irrelevant. Further they come to the conclusion that the successive application of CAESAR with keys i and j results in a single CAESAR encryption with the key $i + j \bmod 26$. Hence, the number of different keys is small enough to check all of them within 3 days.

Step 8: A Monoalphabetic Cryptosystem. Now, we look at a better cryptosystem, called the MONOALPHABETIC cryptosystem, it is similar to CAESAR. Again, every character is replaced by a different character, but instead of shifting the characters by a fixed number of positions, we jumble the characters arbitrarily (i.e. we take a permutation of the characters):



How many keys do we have now? $26! \approx 4.03 \cdot 10^{26}$ and this is a huge number. Nobody is able to check so many keys within reasonable time. But can one exclude another possibility to break a cryptotext that is encrypted with this cryptosystem? Many students discover by their own how the cryptanalysis works: In every language, some of the characters appear more often than other characters. In German, for example, E is the most frequent character followed by N and I. Comparing the frequencies of the letters of a given cryptotext to the expected statistical distribution provides us with a hint for the cryptanalysis. Additionally, we can pay attention to some words that occur often in texts, such as *und* or *das* in German.

It is important though that this frequency analysis only works reliably for large cryptotexts. For the students, a text should be provided that is not too long, but in which the frequencies of the characters more or less coincide with the expected statistical distribution. Tables of these distributions are given for example by Wätjen [14] for German and English.

Step 9: A Longer Exercise. Now, it is time for a longer exercise. The students form groups of two or three people and every group gets a print-out of a table

with the expected letter frequencies and a cryptotext, which is a monoalphabetic encryption of a German text. We use the following text [6] at schools[2]:

```
HOQ HQKSD, DOCOPTSPXXO KERJEHOLZOS, PXN PT VOXOS
HOX TOSXLCOS NPOR OPSDOVEQJOIN; XLCMS HPO
OPSRKLCXNO SOEDPOQ WOQECN UK KER HOQ KEXXPLCN, OPS
VPXXOS JE NOPIOS, HKX KSHOQO ESX YMQOSNCKINOS.
OPSPDO XPSH DIEOLZIPLC DOSED, OPSOS WOQER JE
RPSHOS, HOQ PS HOQ IMOXESD YMS QKONXOIS WOXNOCN.
KWOQ HPO TOPXNOS YMS ESX TEOXXOS HPOXOS HQKSD TPN
HOQ IMOXESD ZEOSXNIPLC JE ESXOQOQ ESNOQCKINESD
KEXDOHKLCNOQ QKONXOIKERDKWOS XNPIIOS.
HONOZNPYDOXLCPLCNOS ESH ZQOEJVMQNQKONXOI VOQHOS
YPOIOS SENJOS; OPSPDO VOSPDO TMODOS XPLC HOQ
OSNXLCIEOXXOIESD YMS DOCOPTXLCQPRNOS CPSDOWOS.
```

Most of the students need between 20 and 30 minutes to break this text. Those groups are successful, which divide the work in reasonable parts. It is not necessary to count all the characters. Sometimes it is sufficient to determine what E, N and I are and then you may see some patterns from words that you know. The best way to break it is possibly a mixture between counting the characters and searching for known patterns. The students choose this way intuitively.

In this exercise, the students can live out their curiosity for puzzles. We observed that also students that are usually not easy to motivate for informatics like this type of exercise. Because they are in the position of the cryptanalyst and some minutes ago the task seemed to be unsolvable, their ambition to break the cryptotext is really high.

It is important that we do not break off the exercise sessions until at least half of the students finish their work and almost everybody understands how to break the cryptosystems or to solve the exercise. Usually, most of the students finish the cryptoanalysis approximatly at the same time. If this is not the case, you can give the faster students more challenging exercises to solve until the others are finished. Also, if some of the students have already found the solution, the other students are still eager to break the cryptotext on their own. Sometimes we offer prizes for the first groups who break the text but even if there is nothing to win, the students are willing to solve the exercise.

Steps 1 to 6 are strongly teacher leaded parts. The teacher presents the cryptosystems and the students try to find together the weeknesses of the systems. From Step 7 on, the students work for the most time for themselves and in smaller groups. They need much more time for the last three steps.

In most classes, we need 90 minutes up to this point. It is not unusual that some classes are faster. We were able to give them also a short overview of polyalphabetic cryptosystems.

[2] To make the task easier, we do not take out the punctuation marks and the blanks.

3.3 Continuing Lessons

The search for a secure cryptosystem continues. The first measure of the code designers was to build cryptosystems with more and more keys. The monoalphabetic cryptosystem has a lot of keys, but we were still able to break the cryptotexts with a frequency analysis. The problem was that the frequencies of the characters in the plaintext are a permutation of the frequencies of the characters in the cryptotext. Is there a possibility to mask those frequencies in the cryptotext? One possibility is to use *polyalphabetic cryptosystems*. One example is the cryptosystem VIGENÈRE. The sender and the receiver must agree on a keyword, which is written from left to right multiple times without a gap underneath the plaintext. Every character of the plaintext is encrypted with the cryptosystem CAESAR: The rank of the character in the alphabet of the keyword underneath the character of the plaintext determines the shift. Hence, it depends on the position of the character in the plaintext, with which shift it is encrypted.

VIGENÈRE was invented around 1550 and named after Blaise de Vigenère. At that time, it was considered as unbreakable. Not until 300 years later, Charles Babbage managed to break this cryptosystem: For a key length n, he divided the cryptotext in n parts such that the characters in every part were encrypted with the same shift. Then, every part can be tackled with the frequency analysis. For this analysis, we have to assume that we know the length of the key. However, there are also methods to determine the key length (see [6,13]).

If the teacher only wants to give an overview to cryptology, he can outline public-key cryptology instead. A teaching unit as well as its scientific background is, for example given by Keller et. al. [9] (cf. [2,12]).

4 Experiences

We were teaching this lesson in about 20 schools in Switzerland. In the majority of cases, the schools invited us for a workshop, where this lesson was only a small part of the day. But we have also given short talks about this topic.

The last lecture before school holidays is always a special one. On one hand, the students are tired from the semester. On the other hand, they look forward to the school-free time and they are excited. Hence, it is a special challenge for the teacher to choose a topic which is interesting enough to elate the students in this situation.

In January 2011, we performed the presented lesson at a high school in Zurich in the framework of a regular informatics course. The lesson was for a programming class (in 10th school year, ages 17 to 18) and it was the last lecture before holidays. We wanted to give the students some insights to an interesting and important topic. Altogether we had 53 students.

A question which arose from time to time during the semester was, why is informatics important for everyday life. The goal was to show with this sample lesson the importance of informatics using cryptology as an example.

We aimed to create a lesson which elates all students, even those who are not very interested in informatics.

4.1 Evaluation

Influencing or changing students' attitudes to school subjects is generally a very hard objective, even when teaching classes over a very long time. Since attitudes are difficult to observe or to quantify, gaining evidence of a change in the way students think about a specific matter is a complex task, requiring formal empirical tests and deep know-how in cognitive psychology. The short survey we are going to present and to discuss aims to help confirming or rejecting the impression we had during the lecture. It clearly does not fulfil the requirements of a formal empirical study.

We were interested, whether this short introductory lesson into cryptology has an effect on the opinion of the students. Therefore we conducted a post-questionnaire four weeks after this introductory lesson took place. 53 students had to rate six statements with a rating between "total agreement" (rated 5) to "total disagreement" (rated 1). This questionnaire is not meant to be a full evaluative test, but merely a way to get some feedback (see Fig. 2).

The first question covered the previous knowledge about the topic. On average, this question was rated with a 2.5, which is higher than we expected. This could indicate that the topic is interesting enough, so that the students had already read something about it. A questionnaire from a comparable group of students showed that 50 % of them did not know the meaning of the expression "cryptology". In that group we had 87 students. One possible explanation of the relatively high value in this study is that the students were familiar with the term "cryptology".

With the second statement, we wanted to know whether we did a good job on getting the attention of the students. With an average rating of 4, the students attested that the instruction was indeed interesting, none of them answered that it wasn't interesting at all and 80 % rated the statement higher than 3. Certainly we hope that we did a good job, but we also believe that this in part means that cryptology is indeed an interesting subject.

The third point stated: "I would like to know more about the topic". 70 % answered that they agree or totally agree with this statement. Only six students do not want to know more about the topic. As this question was also answered very positively, we hope that the student's interest is strong enough that they might conduct some further reading on their own.

With statement 4, we wanted to find out whether the students believe that cryptology is indeed used in real life rather than just being a theoretical toy. Although the average of 3.8 is quite high, we think we could do better here. The quite similar statement 5 was on the other hand answered with much more agreement (average 4.3). It is good to see that the students approve that cryptology is important for today's communication. Possibly the previous question was rated lower because none of the students has ever used cryptology outside of school.

We are surprised with the outcome of the last statement. We hoped that the students would agree much more with this proposition. However, the question is

formulated very vague. If the statement would have been "Everyone should know that cryptosystems exist and can protect your data" for example, the answers would probably look quite different.

The most important conclusion we made is, that after a few weeks, the students still remember this lecture. This topic is strongly related to their real life and therefore, this lecture seemed to influence the students attitudes towards informatics. Although, this lecture was meant to be only a short overview, some knowledge transfer happened.

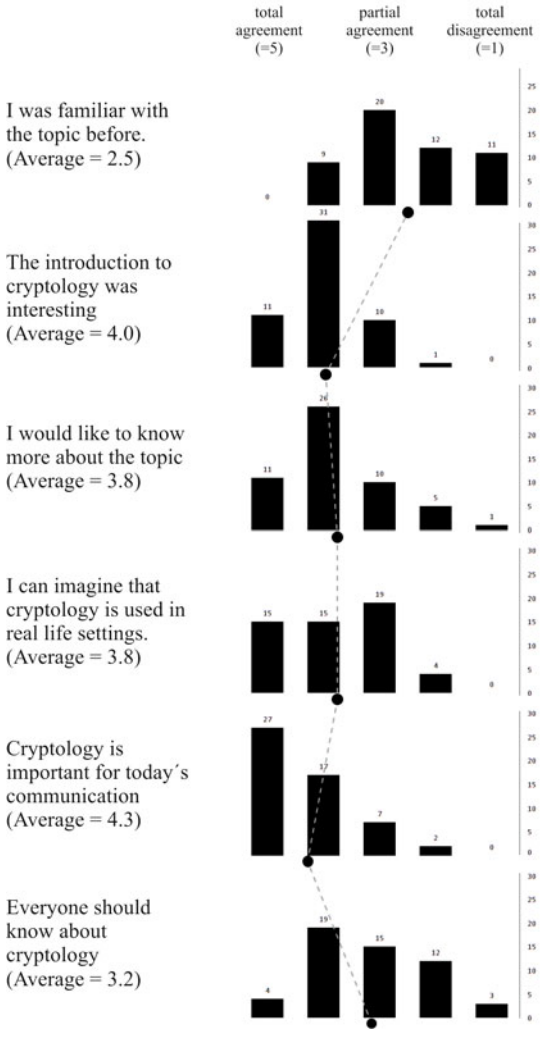


Fig. 2. Chart showing the graphically prepared data

5 Conclusion

In this paper, we introduced a classical cryptology lesson in which the students take the position of the cryptanalyst. The teacher takes the role of the code designer and presents the students some cryptosystems, and the students try to break these systems. Students are able to do that and this gives them a feeling of success. Also, the interesting history about cryptology motivates the students for further cryptology lessons.

This sample lesson can of course also take place in a math class since cryptology is a topic strongly related to both mathematics and informatics.

References

1. Bauer, F.L.: Decrypted Secrets: Methods and Maxims of Cryptology, 4th edn. Springer, Heidelberg (2006)
2. Bell, T., Fellows, M., Witten, I.H.: Computer Science Unplugged - Off-line activities and games for all ages (1999), `http://www.csunplugged.org`
3. Beutelspacher, A.: Cryptology. Mathematical Association of America, Washington, DC (1994)
4. Bruss, D., Erdélyi, G., Meyer, T., Riege, T., Rothe, J.: Quantum cryptography: A survey. ACM Comput. Surv. 39 (July 2007)
5. Freiermuth, K., Hromkovic, J., Steffen, B.: Creating and testing textbooks for secondary schools. In: Mittermeir, R.T., Sysło, M.M. (eds.) ISSEP 2008. LNCS, vol. 5090, pp. 216–228. Springer, Heidelberg (2008)
6. Freiermuth, K., Hromkovič, J., Keller, L., Steffen, B.: Einführung in die Kryptologie. Vieweg+Teubner (2009)
7. Hromkovič, J.: Sieben Wunder der Informatik. Vieweg+Teubner (2008)
8. Hromkovič, J.: Algorithmic Adventures. Springer, Berlin (2009)
9. Keller, L., Komm, D., Serafini, G., Sprock, A., Steffen, B.: Teaching public-key cryptography in school. In: Hromkovič, J., Královič, R., Vahrenhold, J. (eds.) ISSEP 2010. LNCS, vol. 5941, pp. 112–123. Springer, Heidelberg (2010)
10. Kerckhoffs, A.: La cryptographie militaire. Journal des sciences militaires IX, 5–38 (1883)
11. Kerckhoffs, A.: La cryptographie militaire. Journal des sciences militaires IX, 161–191 (1883)
12. Koblitz, N.: Cryptography as a teaching tool. CRYPTOLOGIA: Cryptologia 21(4), 317–326 (1997)
13. Singh, S.: The Code Book. Doubleday (1999)
14. Wätjen, D.: Kryptographie. Springer, Heidelberg (2008)