Using cryptology to teach fundamental ideas of mathematics

Thomas Borys

ABSTRACT

Cryptology is a very old science and until a few decades it was a science for government, military, secret services, and spies. Nowadays, cryptology is almost everywhere in our lives. This article reports on an epistemological analysis of the question: "Is it possible to teach fundamental ideas of mathematics by using cryptography?" In a first step fundamental ideas of mathematics, which are the basic guidelines for mathematical education are discussed. For the analysis a set of fundamental ideas of mathematics is developed e.g. algorithm, functional dependence, modelling, number, measuring, and ordering. In a second step connections between the set of fundamental ideas and various techniques of cryptology are shown. Some outstanding examples for this part of the analysis are the Fleissner grille or the Diffie-Hellman key exchange.

Keywords: Cryptology. Mathematics Education. Modelling. Fleissner grille. Diffie-Hellman key exchange.

Usando criptologia para ensinar ideias fundamentais de matemática

RESUMO

Criptologia é uma ciência muito antiga e, até algumas décadas, era uma ciência para o governo, forças armadas, serviços secretos e espiões. Hoje em dia, criptologia está quase em toda parte em nossas vidas. Este artigo relata uma análise epistemológica da pergunta: "É possível ensinar ideias fundamentais da matemática, usando criptografia?" Em uma primeira etapa, ideias fundamentais da matemática, que são as diretrizes básicas para a educação matemática, são discutidas. Para a análise, um conjunto de ideias fundamentais da matemática é desenvolvido, incluindo, por exemplo, algoritmo, dependência funcional, modelagem, número, medição e ordenação. Em uma segunda etapa, conexões entre o conjunto de ideias fundamentais e várias técnicas de criptologia são mostradas. Alguns exemplos notáveis para esta parte da análise são a Grade Giratória de Fleissner ou a Troca de Chaves de Diffie-Hellman.

Palavras-chave: Criptologia. Educação Matemática. Modelagem. Grade Giratória de Fleissner. Troca de Chaves de Diffie-Hellman.

WHY IS CRYPTOLOGY SO IMPORTANT?

Since the existence of humanity people have always the need to communicate confidentially with each other. Nobody should understand the communication or even don't know that the communication is in progress. So cryptology is a very old science.

Thomas Borys is Doctor in Mathematics. Professor in Institut für Mathematik und Informatik der Pädagogischen Hochschule Karlsruhe – Germany. Adress: Bismarckstrasse 10. 76133 Karlsruhe - Germany.
E-mail: borys@ph-karlsruhe.de

Recebido para publicação em 12/09/2016. Aceito, após revisão, em 13/10/2016.

In the history of cryptology, there are many funny examples of secret communications. For example, Herodotus tells one case. Histiaeus (520-493 BC), also called the tyrant of Miletus was captured and imprisoned in Susa. He wanted to send a signal to his son in law Aristagoras for rebellion and freeing himself. So he cut the hair of a slave, then he pricked a tattoo on the head of the slave. Afterwards the slave has to wait till his hair was re-grown, at this time he sent the slave to his son in law. Now the slave went to Aristagoras and nobody was able to see his secret message, because all hair covered the important secret. When the slave arrived at Aristagoras his hair was cut a second time. So Aristagoras read the message, made the rebellion, freed his father in law, but made himself king.

This example shows that cryptology is a very old science. Until a few decades it was a science for government, military, secret services and spies. Nowadays, cryptology is almost everywhere in our daily life. For example:

- login at the E-mail Account,
- working on a https-Server, for example online banking,
- all cards in our pockets are full of cryptology, credit cards, calling cards and so on,
- mobile phones need many applications of cryptology, for example the GSM-Standard for ciphering phone calls,
- car keys for opening the car,
- or RFID's (Radio-frequency identification), for example books in the library are signed with this tags.

These examples show the importance of cryptology in our daily life. So we see cryptology is nearby everywhere. All modern cytological applications are working so well because they use a lot of mathematics. But mathematics is hidden by the technology. So, for a modern math-education we should recover mathematics in modern technology and show that mathematics is a high-tech science. But in which way should we do this? For an epistemological answer of this question we use the fundamental ideas of mathematics.

FUNDAMENTAL IDEAS

The principle that math education should be led by fundamental ideas goes back to the beginning of the 20th century. Alfred North Whitehead was one of its famous devotees. In his “INTRODUCTION TO MATHEMATICS” he states: “The study of mathematics is apt to commence in disappointment” (WHITEHEAD, 1924, p.8). Whitehead notice the cause that “the pupils are bewildered by a multiplicity of detail, without apparent relevance either to great ideas or to ordinary thoughts. The extension of this sort of training in the direction of acquiring more detail is the last measure to be desired in the interest of education” (WHITEHEAD, 1970, p.119).

Thus he proclaims: “The science as presented to young pupils must lose its aspect of reconditeness. It must, on the face of it, deal directly and simply with a few general ideas of far-reaching importance. ... For the purposes of education, mathematics consists of the relations of number, the relations of quantity and the relation of space" (WHITEHEAD, 1970, p.119). In another section he added the fundamental idea of functionality (WHITEHEAD, 1970, p.125).

The American psychologist Jerôme Seymour Bruner (born 1915) is another very important person in this context. In his book "The Process of Education" from 1960, he writes: "It is simple enough to proclaim, of course, that school curricula and methods of teaching should be geared to the teaching of fundamental ideas in whatever subject is being taught" (BRUNER, 1960, p.18). He does not define the term of fundamental ideas because he uses different terms: *basic and general ideas* (BRUNER, 1970, p.17), *fundamental structure of a discipline* (BRUNER, 1970, p.25), *fundamental principles and ideas* (BRUNER, 1970, p.25). All terms have essentially the same meaning. Bruner concentrates the following items of fundamental ideas for math education, which are not complete. ”If the understanding of number, measure and probability is judged crucial in the pursuit of science, then instruction in these subjects should begin as intellectually honestly and as early as possible in a manner consistent with the child's forms of thought“ (BRUNER, 1966, p.53).

The aim of this article is to examine if the contents of cryptology allows teaching fundamental ideas of mathematics. So sets of fundamental ideas of mathematics are needed. In the German mathematics didactics sets of fundamental ideas are of particular interest. Therefore, the researchers draw up many catalogues of fundamental ideas (SCHWEIGER, 2006). In Table 1 some important catalogues are listed for overlooking many years of discussion. The catalogues of Schreiber, Tietze/Klika/Wolpers and Heymann are chosen because they contain the entire mathematics. The catalog of Humenberger/Reichel is chosen because this catalog is special for the applied mathematics.

TABLE 1 – Different catalogues of fundamental ideas of mathematics.

Schreiber	Tietze/Klika/Wolpers	Humenberger/Reichel	Heymann
1. algorithm	1. algorithm	1. models, language and translation processes	1. number
2. exhaustion	2. approximation	2. approximation method, approximate values and error control	2. measuring
3. invariance	3. function	3. stochastic	3. spatial structuring
4. optimality	4. modelling	4. optimize	4. functional dependence
5.function	5. geometrization	5. algorithms	5. algorithm
6. characterisation	6. linearization	6. represent situations with a mathematical view	6. modelling
		7. networking of mathematical facts	

Source: Borys (2011, p.165).

The fundamental idea of algorithm is common in all sets. Modelling or model and function or functional dependence are parts of three of four sets. So one sees the importance of these fundamental ideas. For the purpose, to examine whether cryptology carries fundamental ideas of mathematics, the following ideas are selected: algorithm, functional dependence, modelling, number, measuring, ordering (means the geometrical classification and the logical ordering). Number, measuring and ordering are chosen, because they cover the other ideas (see BORYS, 2010, p.36).

CRYPTOLOGY IN THE VIEW OF THE FUNDAMENTAL IDEAS OF MATHEMATICS

What is cryptology? The Encyclopædia Britannica (2002) writes: “cryptology, science concerned with communication in secure and usually secret form. It encompasses both cryptography and cryptanalysis. The former involves the study and application of the principles and techniques by which information is rendered unintelligible to all but the intended receiver, while the latter is the science and art of solving cryptosystems to recover such information”. Thus cryptology is a very wide field so this article will focus only on cryptography.

The plaintext is the message that will be put into a secret form (KAHN, 1996, p.xv). The message maybe hidden in two basic ways, the methods of steganography and or cryptography. The methods of steganography conceal the very existence of the message, like invisible ink, microdots, secret compartment or the example of the slave. The methods of cryptography don’t conceal the presence of the message but render it unintelligible to outsiders by various transformations of the plaintext. In cryptography two basic methods of transformations exist, the transposition and the substitution. In transposition the letters of the plaintext are jumbled; their normal order is disarranged. For example, take the Name “Edgar Allan Poe” and jumble the letters and get “der analoge Alp”. This sounds very funny in German, the meaning being “the common joker”. The mathematical concept behind this is a permutation of the letters. For example,

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 1 & 10 & 5 & 3 & 4 & 7 & 8 & 14 & 13 & 6 & 12 & 15 & 9 & 11 \end{pmatrix}$$

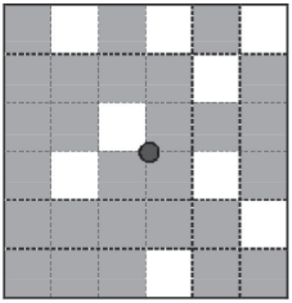
With the substitution the letters of the plaintext are replaced by other letters, numbers or symbols etc. For example, in the name “Edgar Allan Poe” all letters are substituted by his following letter in the alphabet, so you get “Fehbs Bmmbo Qpf”, which is also not readable.

Now it is time to examine two outstanding examples. The first example is the Fleissner grille which works with transpositions and uses the mathematical concept of rotation. The second example is the Diffie-Hellman key exchange because it is a system which everyone uses every day, it is pure math and it is the easiest public key cryptosystem.

Fleissner grille

Eduard Fleissner of Wostrowitz describes in his manual to cryptography by 1881 (original title: “Handbuch zur Kryptographie”) turning encryption grilles. With these grilles he creates a permutation of letters of a plaintext. Even Archduke Rudolf (1858-1899) son of Franz Joseph I (1830-1916) Emperor of Austria encrypted his letters because he didn’t want that his father gets notice of his liberal views (for an example see BORYS, 2011, p.272). The Fleissner grille was really in use, with this example you teach real history. Fleissner works in his book with 5x5, 7x7 and mostly with 15x15 grids. For pupils it is easier to work with grids which have an even number of rows and columns because then the centre of the grid is formed by the crossing of the centre lines which is the turning centre. A suitable example is published from the novelist Jules Verne in his novel “Matthias Sandorf”. This grille is made by a 6x6 grid with 9 holes. Some cells are covered. They are black in figure one; the white one´s are holes of the grille.

FIGURE 1 – 6x6 turning encryption grille.



Source: Verne (1986).

For encryption place the template on a sheet of blank paper. The best is when one takes a sheet of the same size like the template, draw a grid of the same size onto the paper and place them straight together. Now write letter by letter into the holes, only one letter of the plaintext into every hole. If the blanks are filled in the template so rotate it around its centre by 90° and new free fields will appear. Fill in the free fields. Fleissner gives the hints, to hold the grille firmly, don’t displace it, don’t skip any hole. Repeat this twice then the grid is totally filled. If the plaintext is too short so fill in the remaining blanks with meaningless letters. If the plaintext is too long you have to use a second square and repeat it all. Finally, the whole grid is filled in and you get the cipher text by reading out the grid letter by letter and row by row.

Which fundamental ideas of mathematics may one may teach with Fleissner grilles?

One can easy illustrate the fundamental idea of algorithm with it. A nice model for showing this is to describe the process of encryption and decryption with the Input-Process-Output Model.

Encryption

Input: Plaintext

Process: 1. Lay the grille onto a sheet of paper and fill in sequentially the blanks of the grille with letters of the plaintext.

2. If the blanks are filled in the template so rotated it around its centre by 90° and new free fields will appear. Fill in the free fields.

3. Step 2 is twice more repeatable till the entire square is filled. If the plaintext is too short so fill in the remaining blanks with a meaningless string of letters. If the plaintext is too long you have to use a second square and repeat step 1 to 3.

Output: The cipher text is read row by row.

Decryption

Input: Cipher text

Process: 1. Fill in the cipher text letter by letter and row by row in a table (mind its size).

2. Lay the grille over the filled table (mind the starting position of the grille).

3. Read all letters which appear in the blanks of the grille.

4. Turn it around its centre by 90° (mind the direction of rotation). Finally read again.

5. Step 4 is twice more repeatable then you have all letters of the square. If some letters of the cipher text remaining, repeat step 1 to 4 until all letters are deciphered.

Output: Plaintext

With the Fleissner grille it is also possible to illustrate the fundamental idea of functional dependence. The idea of encryption with turning grilles is to make a permutation of all letters of the plaintext. This permutation is set by four parameters: size of the grille, position of the holes, position of laying up the grille and direction of rotation (clockwise or anticlockwise), e.g. for this grille see Figure 2.

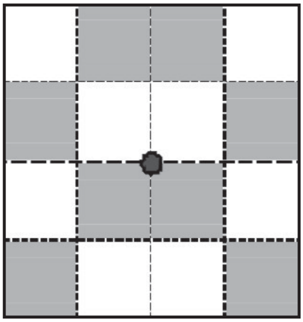
FIGURE 2 – Permutation of the grille of figure one.

Position in plaintext	1	2	3	4	5	6	7	8	9	10	11	12
Position in cipher text	2	4	6	11	15	20	23	30	34	1	5	8
Position in plaintext.	13	14	15	16	17	18	19	20	21	22	23	24
Position in cipher text	10	13	18	21	25	28	3	7	14	17	22	26
Position in plaintext	25	26	27	28	29	30	31	32	33	34	35	36
Position in cipher text	31	33	35	9	12	16	19	24	27	29	32	36

Source: The author.

The fundamental idea of ordering can be illustrated in different ways with the Fleissner grille. The essential idea of turning grilles is the rotation of the grille and rotations are mathematical concepts. Figure 1 shows a grille which is working with three rotations. Figure 3 shows a grille which is working only with one rotation by its centre by 180°.

FIGURE 3 – 2x2 turning encryption grille.



Source: The author.

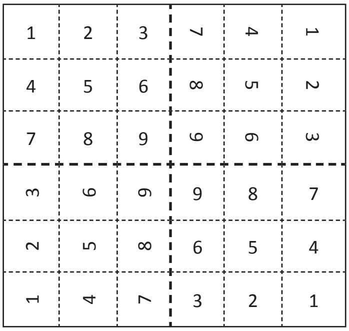
What is therefore interesting for teaching?

It is very well possible to train mathematical problem solving skills within this context. For example by solving the following problems:

- Produce a working Fleissner grille.
- In which way do you build up a working Fleissner Grilles?
- How many different 4x4 or 6x6 or (2n)x(2n) Fleissner templates exist?

Answers of these questions are easy when you enumerate the grille of figure one by 1 to 9 (see figure four). For a working grille only one cell of each number is taken out. For every cell you have 4 different opportunities. Thus for the 4x4 type $4^4=256$ different templates are existing, for the 6x6 type $4^9=262,144$ and for the (2n)x(2n) type exist 4^{n^2}.

FIGURE 4 – Numbered 6x6 grid.



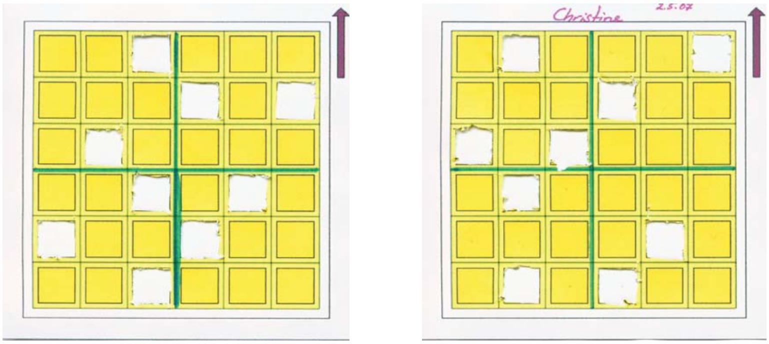
1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Source: The author.

For teaching at the elementary school, it is recommended to work with a 4x4 grille, because the handling is easier and the students have no problems to overlook all cells, letters, turns and so on. Some gifted students maybe work with the 6x6 grille.

The author worked with children in secondary schools of different ages. Figure 5 shows some grilles which are made by a girl at the age of 13 years. The left picture shows a grille, which doesn't work because there are some holes in the wrong cell. The grille on the right is working, because every hole has a unique number (see figure five).

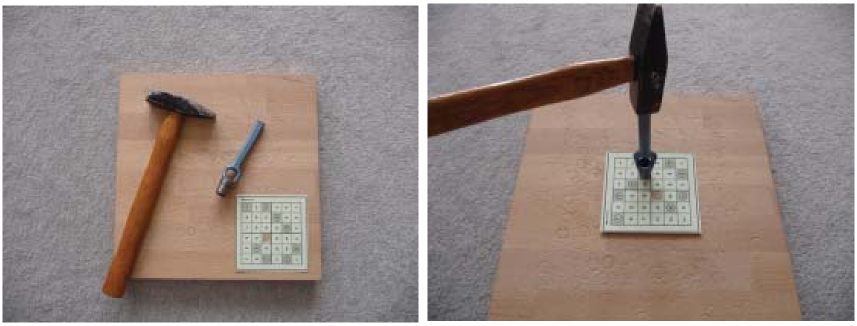
FIGURE 5 – Fleissner grilles produced by a girl at the age of 13 years.



Source: The author.

In this stadium of my studies the children produced the holes with scissors or cutters. Producing the holes in this way is very exhausting. A better way is to work with a stamp. With a stamp, a hammer and a wood pad you only need seconds to cut out the holes (see Figure 6). Another solution for the cutting problem is to use a punch.

FIGURE 6 – Tools for producing quickly Fleissner grilles.



Source: The author.

Diffie-Hellman key exchange

Diffie-Hellman key exchange is invented by Whitefield Diffie and Martin Hellman. They published it 1976 with their paper “New Directions in Cryptography”. It allows two parties that have no prior knowledge of each other to share a secret key over an insecure communication channel. Which fundamental ideas of mathematics may you teach with the Diffie-Hellman key exchange?

One can illustrate the fundamental idea of algorithm with it. For example, one call the two parties who like to exchange a key Alice and Bob.

Input: Over an insecure canal Alice and Bob communicate two numbers:

1. a prime number q
2. a generator g ($2 \leq g \leq q$-2) which is a prime root of q.

Process: Alice chooses $\alpha \in \{1, ..., q\text{-}\}$, computes $\alpha = g^a \bmod q$ and sends α to Bob.

Bob chooses $b \in \{1, ..., q\text{-}\}$, computes $\beta = gb \bmod q$ and sends β to Alice.

Output: Alice computes $K = \beta^\alpha \bmod q$.

Bob computes $K = \alpha^b \bmod q$.

Both get the same key.

The key K is the shared secrete of Alice and Bob, only they know it. An observing third person is not able to compute the key, if Alice and Bob choose q as a large prime number about a length of 1000 bit and more. Mathematics guarantee that nobody is able to calculate K, if he has only the information about (q, g, α, β). For computing a or b you have to solve the equation $\alpha = g^a \bmod q$ or $\beta = g^b \bmod q$, but this problem is known as the discrete logarithm problem. For solving this problem no efficient algorithm is known. Exactly this point is the core of mathematical modelling, because the mathematics ensures that the communication is secret.

So with the Diffie-Hellman key exchange it is easy to illustrate the fundamental idea of mathematical modelling. This method of key exchange is applicable in all types of client-server environments. Thus, client and server use the Diffie-Hellman key exchange to arrange a secret key. After that client and server encrypt information by using the exchange key. The SSL protocol which is used on the Internet at the pages marked with HTTPS works in this manner.

Fundamental idea of number has a centre role in the Diffie-Hellman key exchange. Let’s make an example by using small numbers for illustration:

Alice and Bob arrange

q=97 g=23

Alice chooses a=20 and computes: Bob chooses b=31 and computes

$\alpha = 23^{20} \bmod 97$=43 $\beta = 23^{31} \bmod 97$= 87

Exchange of α and β

Alice computes: Bob computes:

$K = 87^{20} \bmod 97$=73 $K = 43^{31} \bmod 97$=73

The common secret key is K=73.

Some aspects about the needed numbers:

- For the first number q one needs a prime number.

- For the second number one can choose any g, such that g is primitive to mod n and there is no reason why not choosing the smallest g you can – generally one-digit number (SCHNEIER, 1996, p.514). In school one do not need a prime root of q to work with the Diffie-Hellman key exchange because g does not have to be primitive, it just has to generate a large subgroup of the multiplicative group mod n (SCHNEIER, 1996, p.514).

- With a standard school calculator, one may get problems to compute some exponents because it is not possible to type this in with one step. One needs several steps by using exponentiation by squaring and the modular arithmetic. If one would like to avoid this just work e.g. with the calculator of windows or CAS.

The two examples Fleissner grille and Diffie-Hellman key exchange show that it is very interesting to examine the illustration capability of cryptology concerning the fundamental ideas of math. Furthermore, other useable examples are: The Greek skytale, the Roman Caesar code, the Vigenère code, the RSA code, etc. All these examples are presented in Borys (2011).

REFERENCES

BORYS, T. Using Codes to Teach Fundamental Ideas of Mathematics. *The International Journal of Learning*, v.17, n.6, p.33-42, 2010.

BORYS, T. *Codierung und Kryptologie*. Wiesbaden: Vieweg+Teubner Verlag, 2011.

BRUNER, J. *The Process of Education* (10th ed.). Cambridge MA: Harvard University Press, 1966.

DIFFIE, W.; HELLMAN, M. E. New Directions in Cryptography. *IEEE Transactions on Information Theory*. Institute of Electrical and Electronics Engineers, v.22, n.6, p.644-654, 1976.

FLEISSNER von WOSTROWITZ, E. *Handbuch der Kryptographie.* Wien: K. k. Hofbuchdruckerei Carl Fromme, 1881.

KAHN, D. *The Codebreakers*. New York: Scribner, 1996.

SCHNEIER, B. *Applied Cryptography*. New York: John Wiley & Sons, 1996.

SCHWEIGER, F. Fundamental Ideas. A bridge between mathematics and mathematical education. In: MAASZ, J.; SCHLOEGLMANN, W. (Eds.). *New Mathematics Education Research and Practice*. Rotterdam, The Netherlands: Sense Publishers, 2006. p.63-73.

VERNE, J. *Mathias Sandorf*. Munich: Deutscher Bücherbund, 1986.

WHITEHEAD, A. N. *An Introduction to Mathematics*. London: Williams and Norgate, 1924.

WHITEHEAD, A.N. *The Aims of Education*. London: Ernest Benn limited, 1970.