Riv. Mat. Univ. Parma, Vol. **14** (2023), 249-264

Aaron Gaio

A cryptography teaching-learning sequence for high school and the concept of public-key cryptography

Abstract. The goal of this paper is to present a teaching-learning sequence about cryptography for high school. Applied discrete mathematics, cryptography in this particular case, is rare to find in the usual school curricula, but can provide good topics for mathematical activities and engage students in a real-world situation. Cryptography is a strongly interdisciplinary subject that would not live without other subjects (most notably, Computer Science, but also Engineering, and so on). Needless to underline the importance of public-key cryptography in the modern world and its application in research and industry and how this contribution can help bridging the gap between school mathematics and the world of research and industry.
The Italian institutional context will be presented, together with a literature review about the teaching and learning of cryptography and discrete mathematics at school. The theoretical framework and methodology used follows the principle of design research and aim at designing and presenting tasks in the model of Realistic Mathematics Education.
After presenting the whole teaching-learning sequence, I will focus on a particular task describing public-key cryptography without the typical use of RSA-like systems.
The teaching-learning sequence and the public-key cryptography activity did respect the principles of RME both in eliciting students' curiosity and interest and in the formation of some initial informal knowledge on the concepts of one-way functions and public-key cryptography that can lead to a more formal mathematical reasoning in future activities.

Keywords. cryptography, public-key, education, school.

Mathematics Subject Classification: 97M10, 97C70.

Received: February 28, 2022; accepted in revised form: October 16, 2023.

1 - Introduction and Context

The paper aims at describing the design and some outcomes of a teaching-learning sequence (TLS, Psillos and Kariotoglou, 2016 [**17**]) about cryptography for high school. This topic can be of interest to students and could engage the learning of some mathematics concepts that are slightly different than the usual topics covered by the curriculum, fostering motivation in the students and a sense of reality of the mathematics learned. The topic has in fact many real-life applications and can help the creation of an idea of mathematics which is less abstract and self-standing if connected to real-world applications.

The European Union, in its recommendations (EU Council, 2018 [**8**]), promotes activities that are integrating areas of the scientific disciplines with their applications in technology and engineering (STEM). They point out the importance of awareness of the question to which mathematics can offer answers, of applying mathematics in everyday contexts and also, more in general, the development of creativity and critical thinking (ibid., 2018). Some important applied mathematics topics arise from these activities, such as ciphers and one-way functions.

What will be presented has been implemented as an activity of the PLS (Piano Lauree Scientifiche) project by a team of the University of Parma at a local high school. The project aims at bridging the gap between scientific faculties in the university and high schools, to help students in the choice of a future path of studies. The class consists of 10th-grade 18 students, who voluntarily participated in the specific mathematics class and therefore quite motivated about the subject.

Section 3.2 will focus especially on one activity of the TLS about graphs and public-key cryptography. The presentation of this activity and relative conclusions will contribute to the a priori and a posteriori analysis of the teaching sequence, with the corresponding implementation.

2 - Literature and Framework

Looking at the past years, some projects concerning discrete mathematics education have been developed around the world, even in lower school grades (works by Hart, 1990; Kenney, 1991; Rosenstein, 1997, Bell, Witten, Fellows, 1998-2015; [**12**], [**13**], [**18**], [**2**]), but this innovation impacted only in sporadic cases the Italian education system.

In fact, some factors as the distance from a traditional school curriculum, a lack of teacher training on the subject and a general uncertainty by teachers about trying new topics in a mathematics area they are not familiar with (Gaio

and Di Paola, 2018 [**10**]), have not made it possible for these discrete mathematics topics to enter the school world with a shared acknowledgement yet. This applies, in the previously cited research to Italy [**10**], as well as to other countries around the World [**18**]. Discrete mathematics is not clearly delimited in our curriculum and teachers are usually not aware that it actually could be.

Going a little bit into detail about the mentioned references, [**12**], [**13**] and [**3**] describe the implementation of Computer Science into the curriculum, emphasizing the algorithms and scientific part of informatics and applied mathematics; [**2**] is really offering some first examples of teaching activities directly design to promote a deep understanding of computer science and mathematics concepts using problems from discrete mathematics and algorithmic thinking.

Among the possible integrated approaches to discrete mathematics from a didactical point of view, this contribution goes in the direction of teaching of informatics as a science (Mirolo, 2003; Bellettini et al., 2014 [**15**], [**3**]), the one that is most related to mathematics aspects.

Some elements of informatics that are strictly connected to discrete mathematics education are present in the school curricula in Italy, as reported in detail by Berrettini et al., 2014 ([**3**]), from which an excerpt: "A fundamental topic shall be the concept of algorithm and algorithmic strategies to solve simple problems for which simple models exist; moreover he or she shall study the concepts of computable function, decidability and related simple examples". The relevance of algorithms in teaching is also stressed recently in mathematics education (Weber et al., 2022, [**20**]; Modeste and Rafalska, 2016 [**16**]).

2.1 - *Literature review on cryptography education*

Most of the work done around cryptography in the Italian school system is related to PLS projects (Piano Lauree Scientifiche, project by universities to connect with high schools) or similar extracurricular projects and activities, still mainly on the last years of high school; some examples are [**1**] or [**6**].

Carried out in many schools all around the country, all projects have a quite similar structure. Topics and activities range from arithmetic in $\mathbb{Z}$, prime numbers, multiple and divisibility, Euclidean algorithm, divisibility rules, modular arithmetics with congruences and congruence classes, operations in $\mathbb{Z}_n$, Fermat's little theorem, and so on. All of this is then applied to build experiences in cryptography such as Caesar's cypher, Vigenére, up to RSA cryptosystem and its functioning as a main example of public key protocol.

A relevant example comes from University of Trieste, that, as a precursor in Italy, developed a project for cryptography in primary school between the 90s and 2002-2003. The proposal was adressed at primary schools also as a mean

to approach statistics; much relevance is given to frequence analysis as a tool to decypher substitution cyphers, or the maximum likelihood model. More details can be found f.e. in [**4**]. The idea of *il gioco dell'agente segreto*, the secret agent game, can be entertaining and engaging for children, while having an impact on knowledges that school brings to the students. Cryptography is well used as a mean of presenting mathematical topics in a way that results fun for students. Many other interesting projects of this kind are carried out, but only a few have repercussions on research in mathematics education, in particular concerning the Italian institutional context.

2.2 - *Theoretical framework and methodology*

In this described context, I felt there was space for some innovation in the presentation of cryptography at high school and need for some mathematics education research contribution to the field. Therefore, a careful design was to be done and an appropriate methodology and framework to be used in order to show the relevance of teaching-learning activities based on cryptography to mathematics learning.

2.2.1 - `Guided reinvention of mathematics and RME`

The teaching methods used in the TLS follow the model of Realistic Mathematics Education [**11**] and Guided Reinvention of mathematics [**5**]. Guided Reinvention of mathematics is based on Hans Freudenthal concept of mathematics as human activity. Education should give students the "guided" opportunity to re-invent mathematics by doing it; focus is on the activity, on the process of mathematization [**9**] . Realistic Mathematics Education (RME) is an instructional design theory which centers around the view of mathematics as a human activity (Freudenthal); "The idea is to allow learners to come to regard the knowledge that they acquire as their own private knowledge, knowledge for which they themselves are responsible" (Gravemeijer) [**11**]. The main goal is to develop a local (i.e. domain-specific) instructional theory (LIT) that will allow students to "*invent* the mathematics themselves" [**11**]. This need two steps: a first one in which "students are engaged in activities designed to invoke powerful informal understandings"; a second one where "students are engaged in activities designed to support reflection on these informal notions in order to promote the development of formal concepts" [**11**].

Design principles in an RME sequence of tasks are:

1. to identify the fundamental concept, potential starting points, and models

that support the learning of mathematics through a phenomenological didactical analysis, thought experiments, discussions with teachers, and working with students;

2. to put model-eliciting activities are at the heart of an instructional sequence. They are cast in contexts that are familiar for students and provide relevant and challenging elements that need to be organized or schematized mathematically so as to have the potential to evoke their (informal) knowledge;

3. to create a task sequence guides students from informal to formal mathematical reasoning. Models play a key role by shifting from a model of a particular situation to a model for mathematical reasoning. Take into account the design of skill development and connections with related mathematical topics to develop strong structures and procedures;

4. to design whole-class and peer-to-peer interaction.

(Kieran et al. [**14**])

2.2.2 - `Design research`

The framework we worked in is that of design research or design experiments [**7**]. For the purpose of this document, the developmental approach is taken into consideration; development studies function is to design and develop a research based intervention [**19**] and constructing design principles in the process of developing it. The principles of design research have been followed in the design of the teaching activity and in the different iterations of it. The goal is to explore new learning and teaching environments, to verify their effectiveness and to develop somehow new methods, instruments and teaching actions to further improve in the field of problem solving and logical thinking, using unusual topics as algorithms and cryptography. Doing this the goal is to contribute to the development of new teaching and learning theories, taking into consideration learning processes in the specific situation, with contents and goals clearly defined. Design research is quite appropriate in this situation, as we are facing a new experience in an environment that we need to analyze carefully, i.e. on a local scale, considering all the different elements in the learning environment. The intended design experiment is a classroom experiment [**19**] in which the researcher (or researchers) cooperates with the teacher in assuming teaching responsibilities. On one hand, the teacher is a part of the design team and will play a key role in the development and reviewing of the activities. On the other

hand, they have no previous knowledge and need a guide to explore the new content to present and during the implementation.

3 - The didactical activity

The TLS proposed consisted of 8 two-hours classes with the described 10th grade class. The TLS was designed using the pronciples of RME in section 2.2.1.

Among the learning goals, there is the learning of some computer science and discrete mathematics concepts:

- *Public-key cryptography and information security* presented in a way that is accessible even for young kids. Focus is on the actual problem of how to send a message without an intruder reading it and many problems connected to it.

- *Algorithms and computational complexity*, with the use of one-way functions, serves as an explanation of how this process works.

3.1 - *Description of the TLS*

The first slot was an introduction to cryptography, cryptology, and various aspect of ancient cryptography. These were presented following the history of the discipline and the progresses made with each new discovery.

In the second lesson, steganography and other historical aspects were presented. After this, the first ciphers were introduced (first basic substitution ciphers such as Atbash cipher or other simple substitution ciphers).

The third lesson was about Caesar's cipher. The method is very simple. You move forward the index of the character in the alphabet and substitute the original character with the one with (shifted, increased) position/index in the alphabet: this way you get the encrypted text. This cipher works by substitution and represent a good introduction to modular algebra. An initial description of the cipher was presented and then students were let free to explore the dynamics of the system from an "intruder" point of view, i.e. trying to break the system and get the meaning of messages that were transmitted. Only after this, some tricks such as letter frequencies and brute force method were explained to the students.

Lesson 4, 5 and part of the 6th were dedicated to the modular algebra behind the Caesar's cipher and its generalization into an affine cipher, a system where each letter is mapped into another letter using a simple mathematical

linear function. Before presenting it formally, some texts and story were given to the students, such as the Gold-Bug by E. A. Poe (see as in Zaccagnini, 2005 [**21**]). The use of these text allows students to connect the various aspects of mathematics and other subjects, such as in this csase literature and provide, in a realistic mathematics education view, with a source of interest and motivation. After such an introduction, the mathematics of affine ciphers and their connection with funcions is finally presented (see Fig. 1). The exercise in the figure is presented in its original form, it is stating that the students need to find two couples x_1, y_1 and x_2, y_2 such that $ax_1 + b = y_1$ and $ax_2 + b = y_2$ to find a and b.

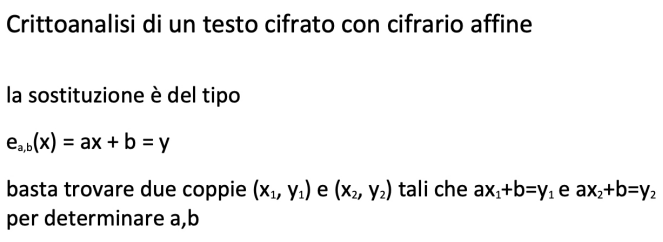

Fig. 1

Attention was posed to the mathematical system to solve the problem of deciphering the messages encripted with this method. Also E. A. Poe's ciphertext can be explained in a substitution cipher approach, that also need some frequence analysis which can lead to even further mathematical background and ideas to develop connected interdisciplinary topics.

The 6th and 7th lesson were used to finally present the difficult concepts of cryptography which is non-private. First of all, a double-lock procedure was implemented with the students, following again the RME ideas, by really locking a box with two different locks. This can provide a first example of cryptography without exchanging a key. Still, this is not public-key cryptography and we need the next activity to present this concept. Public-key cryptography was introduced with an activity inspired by the Computer Science Unplugged project [**2**], using graphs and the definition of a perfect dominating set (see later section).

In the latest lesson, we introduced the RSA-system, after the students were already familiar with the concept of public-key cryptography.

3.2 - *Public-key activity on graphs*

Focus of this section is to present one particular activity of the TLS, namely the PDS of a graph activity on public-key cryptography. We first present some mathematical definitions, and then descrive the teaching activity implemented in the TLS.

3.2.1 - Dominating sets

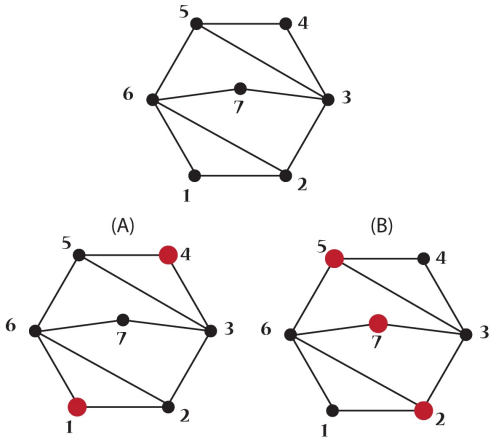

Fig. 2. A graph G. The set of the red vertices in Figure A is not a dominating set for G (since the vertex 7 is not dominated by any of the red vertices); B is a possible dominating set for G.

Definition 3.1. Let $G = (V, E)$ be a graph. A vertex i is said to *dominate* a vertex j if $i = j$ or if E contains an edge from i to j.

A set S of vertices, $S \subseteq E$ is said to be a *dominating set* of G if every vertex of G is dominated by at least one element of S.

Definition 3.2. The set S is called a *perfect dominating set (PDS)* of G if each vertex of G is dominated by at exactly one element of S.

We are then looking for the set of least cardinality among all dominating sets for a graph G.

Given a graph G, is it possibile to find a perfect dominating set for it?

We can try to produce a dominating set (subset of vertices in red) for G as in A in Fig. 3; we will notice how there are vertices that are dominated by more than one red vertex. For example, the two red vertices on the right

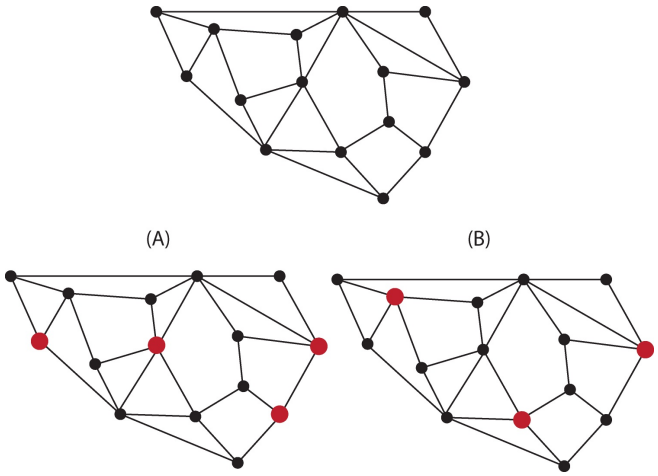

Fig. 3. A graph G and the attempts A and B as described in the example.

of the graph are dominating each other, other then themselves; so the set of red vertices in A is not a perfect dominating set. In example B, each of the red vertices dominate five vertices (four other plus itself), covering exactly the fifteen vertices of G, without any vertex being dominated by two different red vertices. So B is a perfect dominating set for G.

3.2.2 - Description of the public-key activity on graphs

The goal for student A is sending a message to student B in such a way that the conditions of a public key cryptosystem are satisfied, i.e. secrecy is kept, no previous key exchange is needed and only the receiver (the holder of his private key) can decrypt the message. The activity is best done if "student A" and "student B" are groups of students, to better check the computations.

The encryption process works as follows:

- student A receives a graph which will be used for encryption of the message; an example is showed in Fig. 4 (A);

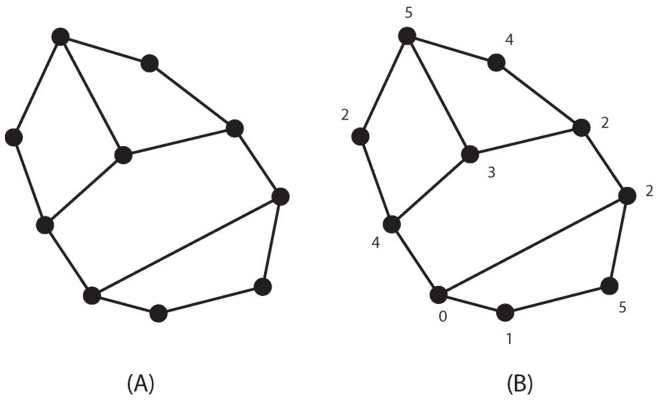

Fig. 4. Encryption of a numerical message, part 1.

- student A wants to send a message to student B, he needs to encrypt it. For our example, the message we are sending is a natural number. So student A chooses a number that is going to be transmitted and write one number for each vertex of the graph (see Fig. 4 (B)). The sum of these numbers is corresponding to the number to be transmitted. In the example the message is $5 + 4 + 2 + 2 + 5 + 1 + 0 + 4 + 2 + 3 = 28$;
- the next step is, for every vertex, adding up the numbers corresponding to the vertex itself, plus all the other vertices of the graph which are at distance at most 1 from the choosen vertex (we obtain the numbers in red in the example in Fig. 5 (A));

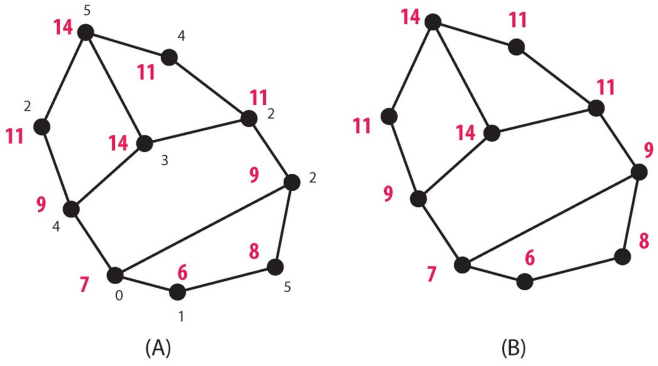

Fig. 5. Encryption of a numerical message, part 2.

- the message is now ready to be sent, transmitting only the red number and not the small ones we started from.

After encrypting the message, the students can exchange their sheets with each other and try to see if they can figure out the others' messages.
To decrypt the message, we need a special private key, which only student B has. With this (see a solution for our example in Fig. 6) it is possible to read the message by just adding up the numbers corresponding to the red dots. So, in the example, we read $11 + 11 + 6$ which is indeed 28 as the message which was sent.

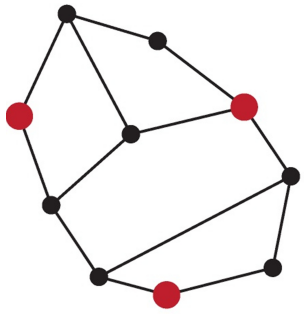

Fig. 6. A decryption key, which is a perfect dominating set for the graph.

Summarising, student B managed to receive a message from student A, without need of key exchange and just by sending a public key (which is in our case the graph), which everyone can see. A possible intruder knows the public key and might even know the encryption process but still cannot access the information in the message.

From this example it is also possible to talk about the idea of a one-way function with the students which are now quite familiar, even if in a very informal way, to computational complexity.

4 - Discussion

As previously mentioned, the TLS was designed using the principles of RME in section 2.2.1.

Principle 1, identifying fundamental concepts (as one-way functions and public-key procedures), are the central goal of the activity on PDS described in details.

Principle 2, regarding modeling and relevance to students, played a central role in the design, as pointed out in the TLS description. Still, questionnaires among the students confirmed this thought, as we will see later.

Principle 4 was intrinsec in the design and methodology as a main portion

of the activities was done as group work with importance in the peer-to-peer interaction.

Can doing something practical and applied, as the TLS proposed, also enhance students' engagement and self-efficacy? Perceived usefulness of mathematics can be improved by some applied mathematics activity? Also, does encouraging discourse in classroom and among students, together with inquiry-based mathematics, proves efficient to create a conceptual understanding in the students? What is the idea of mathematics students have, and can we change it a little?

To explore these questions and hypoteses, we developed a pre and post course questionnaire, which were given to the partecipating students. Notably, some answers changed their points drastically. The questionnaire was on a 5-point or 4-point Likert scale base on some questions and was anonymous. We report some of the most interesting observations from these. Also, informal observation by the resercher and an interview with the teacher was taken into consideration for the following conclusions.

- Question 3 is stating: "*Sono convinto che utilizzero la matematica al di fuori dell'ambiente scolastico*" - "I think that I will use mathematics outside the school enviroment" and got 3.4/5 average score in the pre-course survey and 4.7/5 average in the post-course survey, as a strong sign of perceived usefulness of the applied mathematics tools seen during the lessons. This is also strongly confirmed by the impression of the reseacher and of the teacher on the reaction in the classroom during the lessons. Many interactions with the students regarded curiosities about application of the themes to real-world situations.

- On a similar comparison, Question 5 "*La matematica e importante per la vita quotidiana*" - "Mathematics is important for everydaylife" went from 3.6 to 4.7 (out of 5) and Question 8 "*La matematica serve per far funzionare il mondo*" - "Mathematics is useful to make the World work" went from 3.2 to 4.5.

- On a 4 point Likert scale, Question 2.2, "*Ha cambiato la tua idea di matematica*" - "This activity changed your view of mathematics" had a 3.8/4 average answer, certifying the educational content of the lessons, that are shaping a certain idea of mathematics as a less abstract and more "useful" subject.Also in this case, comments and reactions during the lessons were in the tone of a more "funny" and "engaging" topics than what they were used to in the more formal math classes.

- Self-evaluation by students regarding their learning of new concepts is

also high and got 3.5/4 points average score (the question was direct and asked students if "they learned some new and useful concepts". This was also confirmed by the teacher; from an informal observation of the classroom environment the teacher reports for example, during an interview, a change in the understanding of the public-key functioning, which before "was incredibly difficult to understand" and later "was clear to the students, they were so fascinated by it, they wanted to explain it to classmates and peers". From this last statement is visible also the improved affect and motivation aspects, that were important results.

- Question 2.6 and 2.7 were about future studies in mathematics and students motivation. From the students answers to "did this activity give you a stronger motivation for future studies in STEM disciplines" we got a 3.1/4 and to "will you be more involved in mathematics at school" a surprising high 3.7/4, as a sign of improved motivation in the students.

- Some interesting answers came from the open questions as well, when more students pointed out that they want to share this content with other people and that they were happy they now know the functioning of cryptographic protocols in situation like banks and message transmission they so much use but never think how they really works (messaging social media and bank transaction were mentioned).
  Two students even pointed out in the open questions the fact that this activity increased their motivation to continue and study mathematics in the future.

- A final remark is that the group finally really organized a small math-fair to present some of these topics they learned to friends and family in one of the school open days; we see this as a truthful sign of interest and perceived usefulness of the topics.

5 - Conclusions

The design based methodology and the principles of design research have been followed in the design of the teaching activity and in the different iterations of it. This made a continue review process possible, some fine-tuning of some of the activities after different tryouts. The collaboration with teachers in the design and evaluation of the activities is also worth noticing, since many important feedbacks and comments arose and helped us change and enrich some details of the activity.

Regarding motivation and sense of reality in the students, from the questionnaires, we had confirmation of our hypothesis about the affective aspects, about an increase of motivation in the students, and about an increase of the perceiveness of usefulness that students see in the subject of mathematics.

Learning of new mathematical concepts (and a better process of doing it thanks to the approach) is also of high consideration.

It is again worth noticing how this particular PDS activity explains the concepts of one-way functions and that of public-key cryptography without using, as in most cryptographic examples, notions of modular algebra which would require a lot of time and effort from the students. This made it, in other occasions, possible to present this concept to student with good results in term of understanding of the relatively complex concept. In this case, the conceptualization of the public-key idea is much better even in high school. Later activity regarding RSA showed that students which are more familiar with the public-key functioning can better concentrate on the mathematics content of RSA.

The concept of one-way functions is hard to understand, and therefore, in a vertical perspective, comes easier when faced in more difficult settings, such as RSA, if students are already familiar with it. The idea that it is possible to "work backwards", in the example of the PDS activity starting with a set of vertices which is going to become an efficient solution and generating the general graph. From these remarks, it follows that it is easy to create a public key from a key we already have which can be kept private.

I finally believe that applied mathematics with tools to present it in schools plays an important role, for the reasons stated above, in a changing view of mathematics, not only as a totally abstract subject and a boring repeatedness of rules, but as an engaging and, above all, useful subject for many everyday life situations.

References

[**1**] G. Alberti, *Aritmetica finita e crittografia a chiave pubblica. Un percorso didattico per gli studenti delle Scuole Medie Superiori*, In: A. Abbondandolo, M. Giaquinta, F. Ricci, eds, "Ricordando Franco Conti", SNS, Pisa, 2004, 1–29.

[**2**] T. Bell, I. H. Witten and M. Fellows, *Computer Science Unplugged: off-line activities and games for all ages*, Computer Science Unplugged, 1998.

[**3**] A. Bellettini, V. Lonati, D. Malchiodi, M. Monga, A. Morpurgo, M. Torelli and L. Zecca, *Informatics education in Italian secondary schools*, ACM Transactions on Computing Education (TOCE) **14** (2014), no. 2, 1–6.

[**4**] M. Borelli, A. Fioretto, A. Sgarro and L. Zuccheri, *Cryptography and Statistics: A didactical project*, 2nd International Conference on the Teaching of Mathematics, 2002, 14–16.

[**5**] G. Brousseau, *Theory of Didactical Situations in Mathematics. Didactique des Mathématiques, 1970–1990*, Mathematics Education Library, **19**, Springer Science and Business Media, 2002.

[**6**] A. Centomo, E. Gregorio and F. Mantese, *Crittografia*, 2007.

[**7**] P. Cobb, J. Confrey, A. diSessa, R. Lehrer and L. Schauble, *Design Experiments in Educational Research*, Educational Researcher **32** (2003), no. 1, 9–13.

[**8**] *Council Recommendation of 22 May 2018 on key competences for lifelong learning (Text with EEA relevance)*, Official Journal of the European Union, ST/9009/2018/INIT, OJ C 189, 4.6.2018, 1–13.

[**9**] H. Freudenthal, *Mathematics as an Educational Task*, Reidel, Dordrecht, 1973.

[**10**] A. Gaio and B. Di Paola, *Discrete Mathematics in Lower School Grades? Situation and Possibilities in Italy*, In: E. Hart, J. Sandefur, eds, "Teaching and Learning Discrete Mathematics Worldwide: Curriculum and Research", ICME-13 Monographs, Springer, Cham, 2018, 41–51.

[**11**] K. Gravemeijer, *Developing Realistic Mathematics Education*, CD-ß Press, Freudenthal Institute, Utrecht, 1994.

[**12**] E. W. Hart, J. Maltas and B. Rich, *Implementing the standards: Teaching discrete mathematics in grades 7–12*, The Mathematics Teacher **83** (1990), no. 5, 362–367.

[**13**] M. J. Kenney and C. R. Hirsch, *Discrete Mathematics across the Curriculum, K-12*, Yearbook, National Council of Teachers of Mathematics, 1991.

[**14**] C. Kieran, M. Doorman and M. Ohtani, *Frameworks and Principles for Task Design*, In: A. Watson and M. Ohtani, eds, "Task Design In Mathematics Education: an ICMI study 22", Springer, Cham, 2015, 19–81.

[**15**] C. Mirolo, *Quale informatica nella scuola*, 2003.

[**16**] D. Modeste and M. Rafalska, *Algorithmics in secondary school: A comparative study between Ukraine And France*, CERME10, Feb2017, Dublin, Ireland, 1634–1641, hal-01938178.

[**17**] D. Psillos and P. Kariotoglou, *Theoretical Issues Related to Designing and Developing Teaching-Learning Sequences*, In: "Iterative Design of Teaching-Learning Sequences", Springer, Dordrecht, 2016, 11–34.

[**18**] J. G. Rosenstein, *The Absence of Discrete Mathematics in Primary and Secondary Education in the United States... and Why that Is Counterproductive*, In: "Teaching and Learning Discrete Mathematics Worldwide: Curriculum and Research", ICME-13 Monographs, Springer, Cham, 2018, 21–40.

[**19**] L. P. Steffe, *The teaching experiment methodology in a constructivist research program*, In: M. Zweng, T. Green, J. Kilpatrick, H. O. Pollak, M. Suydam, eds, Proceedings of the Fourth ICME, Birkhäuser, Boston, 1983, 469–471.

[**20**] C. Weber, J. Medova, M. Rafalska, U. Kortenkamp and S. Modeste, *Introduction to the papers and posters of TWG11: Algorithmics*, Twelfth Congress of the European Society for Research in Mathematics Education (CERME12), Feb2022, Bolzano, Italy, hal-03808530.

[**21**] A. Zaccagnini, *Cryptographia ad usum Delphini*, web publication, 2005.

Aaron Gaio
University of Trento
Department of Mathematics
via Sommarive 14
38123 Trento, Italy
e-mail: aaron.gaio@unitn.it