https://doi.org/10.34024/prometeica.2023.27.15302

POSSIBLE DIALOGUES BETWEEN POWER, MATHEMATICS AND CRYPTOGRAPHY

A CRITICAL REFLECTION ON THEIR INTERRELATIONSHIPS

Possíveis diálogos entre poder, matemática e criptografia

Uma reflexão crítica sobre suas inter-relações

Posibles diálogos entre el poder, las matemáticas y la criptografía

Una reflexión crítica sobre sus interrelaciones

Beatriz Fernanda Litoldo
(Universidade Federal do Triângulo Mineiro, Brasil)
beatriz.litoldo@uftm.edu.br

Douglas Ribeiro Guimarães
(Universidade Estadual Paulista, Brasil)
douglas.guimaraes@unesp.br

Recibido: 03/07/2022
Aprobado: 03/07/2022

ABSTRACT

In this text we discuss how power, mathematics and cryptography establish dialogues that are considered critical for the present, but which have influence from the past and concerns for the future. We contextualize our reflections from a historical perspective, especially in the Brazilian context, and advance the debates about how cryptography, based on mathematical theories, influenced and dynamized wars. Going a little beyond this historical context, we present some reflections concerning the role of cryptography as a means of data security, one of the main discussions in contemporary society. In this reflection, we point out the position of power that the holders of this knowledge occupy, and that, in the scope of basic school, lacks important discussions for both teachers and students.

Keywords: cryptography. power. mathematics lessons.

RESUMO

Neste texto discutimos sobre como o poder, a matemática e a criptografia estabelecem diálogos que são considerados críticos para a atualidade, mas que possuem influência do passado e preocupações para o futuro. Contextualizamos nossas reflexões a partir de uma perspectiva histórica, sobretudo no contexto brasileiro, e avançamos nos debates a respeito de como a criptografia, baseada em teorias matemáticas, influenciou e dinamizou as guerras. Indo um pouco além desse contexto histórico, apresentamos algumas reflexões concernentes ao papel da criptografia como meio para a segurança de dados, uma das principais discussões da sociedade contemporânea. Nessa reflexão, pontuamos sobre a posição de poder que os

detentores deste saber ocupam, e que, no âmbito da escola básica, carece de discussões importantes tanto para os professores quanto para os estudantes.

Palavras-chave: criptografia. poder. aulas de matemática.

RESUMEN

En este texto discutimos cómo el poder, las matemáticas y la criptografía establecen diálogos que se consideran críticos para el presente, pero que tienen influencia del pasado y preocupaciones por el futuro. Contextualizamos nuestras reflexiones desde una perspectiva histórica, especialmente en el contexto brasileño, y avanzamos en los debates acerca de cómo la criptografía, basada en teorías matemáticas, influyó y dinamizó las guerras. Yendo un poco más allá de este contexto histórico, presentamos algunas reflexiones sobre el papel de la criptografía como medio de seguridad de datos, una de las principales discusiones en la sociedad contemporánea. En esta reflexión, señalamos la posición de poder que ocupan los poseedores de este saber, y que, en el ámbito de la escuela básica, carece de discusiones importantes tanto para docentes como para alumnos.

Palabras clave: criptografía. poder. lecciones de matemáticas

Contextualizing the discussion

The text presented here originates from the first author's master's work. Having the cryptography theme at the heart of the entire dissertation and taking a qualitative approach, Litoldo's (2016) research, in one of its chapters, paid attention to building a relational dialogue that involved discussions and reflections alluding to the fields of power, mathematics and cryptography.

In the Brazilian context, in general, the topic of cryptography and its possibilities/insertions in Basic Education has been gaining attention, over two decades, in the area of Mathematics Education. As addressed by Litoldo and Guimarães (in press), the literature highlights several studies that focus on establishing dialogues between cryptography and mathematical concepts and/or content, with the aim of presenting teaching proposals aimed at contextualized learning.

Together and in parallel with this scenario, the world has become increasingly globalized and technological. The intense growth of the various means of communication, social media, new ways of doing business, via cyberspace, among others, added to a capitalist system forms, and shapes a new area called 'data security'. Based on complex mathematical concepts, in which cryptography plays a fundamental role, ensuring the confidentiality of information can be considered a representative of power (e.g. economic). However, for some cryptanalysts, breaking these sigils can also represent another type of power (e.g. social).

Having said this introduction, we now invite the reader to embark on the discussions and critical reflections raised by the authors regarding the relational dialogue between power, mathematics and cryptography. The purpose here is not to arrive at an absolute truth or to privilege a perspective of reflection, but, for now, we propose to highlight some of the historical events that allow us to look at the webs established between power, mathematics and cryptography, in the past, at the moment currently and in the future.

Cryptography: initial notes

A long time ago, secret writing was started, having as a necessity the efficiency and secrecy of the administrative communications of the countries and also of the armies. Ensuring messages traveled securely was one of the most important concerns. To prevent messages from being intercepted, several

methods and processes were developed in order to hide the contents. In view of this, the ciphers and codes arise.

In this scenario, some nations created specific departments for codes and ciphers to be produced. On the other hand, the codebreakers, called cryptanalysts, began to strive to unravel what was secret. In this way, the "history of codes and their keys is the history of a centuries-old battle between code makers and decipherers, an intellectual arms race that has had a strong impact on the course of human history" (Singh, 2008, p. 11, our translation).

The remarkable scientific discoveries about the art of secret communication, also known as cryptography, took place in the continuous battle between the creators and the decipherers of ciphers/codes. Ciphers, in search of increasingly secure ciphers/codes, and deciphers, in constant work of breaking, marked history, being important characters in wars and in the results of battles.

In Singh's (2008) view, mathematicians are currently responsible for the battles. According to him, while World War I was marked by chemists (use of mustard gas and chlorine) and World War II by physicists (atomic bomb), it will be mathematicians who, through information, will be in control of the next war weapon. This is because they are responsible for developing ciphers/codes used in the secrecy of military information and, at the same time, they are on the front lines to decode them.

Thus, when studying the evolution of cryptography and understanding how its development was linked to history, it is possible to perceive how power (social, political, economic, scientific, etc.) and mathematics are intertwined. However, the role of this science in information security can make the holders of this knowledge at the forefront of a fundamental process for today's society.

Power, Mathematics and Cryptography

Upinsky (1989), even realizing the whole relationship between mathematics and power, draws attention to how misleading the neutrality of mathematics can be. According to him, it is implicitly present in various sectors of society, masked in the most diverse branches. The author classifies mathematics as a perverse, evil and despotic entity that often disguises itself in a respectable and neutral way. Bauchspies and Restivo (2001), from a sociological perspective of mathematics, also address questions about the supposed purity and naivety of mathematics and establish reflections on 'what do numbers hide?'. As the authors ask the numbers "embedded in networks of power and are they arranged in such a way that they purposely obscure the power behind their visual and oral representations?" (cf. Said, 1983, p. 184 apud Bauchspies & Restivo, 2001, p. 8). In this scenario, according to Skovsmose (2007), some discussions such as the macroeconomic model of a country and flight reservations contain characteristic elements of how mathematics is at work in situations that go unnoticed.

Although mathematics is hidden in the most varied branches of society and its manipulation, a priori, is governed by the interests of a few, Napoleon (1981, apud Upinsky, 1989, p. 30, our translation) argues that "'the pretexts are never lacking for those who they have the power to do what they like' and 'using the supposed principle of general utility as a pretext, one gets as far as one wants'". This assertion reminds us of what D'Ambrosio (1994) comments on the advances we have made in the last century, such as knowledge of nature and the development of new technologies, but which were accompanied by "despicable human behavior", such as the destruction mass, starvation, new diseases, moral decay, etc. And says:

> Much of this paradox has to do with an absence of reflections and considerations of values in academics, particularly in the scientific disciplines, both in research and in education. Most of the means to achieve these wonders and also these horrors of science and technology have to do with advances in mathematics (D'Ambrosio, 1994, p. 443).

Thus, we perceive how numbers have the power to rule the world, having in mathematics the figures that "dance" in the system of power (Upinsky, 1989). But, after all, if numbers rule the world, as Galileo

wanted, anything that exists, in turn, must have a number. In this direction, Upinsky (1989) mentions that, as a result of this principle – numbers rule the world – "not only do all things have number, but also, as [the Pythagoreans] said, 'all things are numbers'" (p. 73, our translation). With this same thought, the author brings Roger Bacon (1214-1294), to argue about the sovereignty of mathematics over all things. According to him,

> Roger Bacon, [repeated] whenever: 'all causes of natural phenomena can be represented by lines, angles and figures' [where he proclaimed that] 'mathematics has universal experiences which apply to all sciences and no science can be understood without mathematics' (Upinsky, 1989, p. 121, our translation).

With this stance, we understand how mathematics, when viewed from the perspective of power, becomes the master of science, assuming great importance in various daily activities of man, being positioned at the core of social development (D'Ambrosio, 1994). Associating this power with cryptography, we observe that its evolution is marked by the search for powerful ciphers, in which mathematics enters its history bringing functions and number theory as excellent tools for secure ciphers (Skovsmose, 2007). To have the mathematics to develop protected ciphers is to have a power of secrecy, which in many cases, such as World Wars for example, is to dominate situations and even influence the course of history (Singh, 2008).

Faced with all this, it is a fact that mathematical thinking and especially its manipulation have intervened throughout history. From this, supremacy consists of understanding the logic of the system and understanding its rules to the point of interpreting and using them in one's favor (Upinsky, 1989). To assimilate this logic is to be aware that whoever wins is the one who ascends the fastest and it is also to understand that this confrontation only generates a greater increase in the organization of power.

For example, the results of wars are nothing more than a reflection of the constant reinforcement of weapons and combat techniques, including the power of secrecy of information (Singh, 2008; Upinsky, 1989). It is from this idea that cryptography and cryptanalysis clash and constantly evolve, because in the same way it is necessary to reinforce and create new encryption and decryption techniques. Thus, from this conception, confrontation alters the balance of power, generating its increase. This example allows us to reflect on the assumption of the ideology of progress, when it considers, assuming as an absolute truth, that scientific, social, cultural development and political progress, among others, are intrinsically related and walk in the direction that the world, at over the course of this development, it can gradually get better. The logic of the system mentioned by Upinsky (1989) opposes this assumption and gives strength to the considerations made by D'Ambrosio (1994) that reflects and conceptualizes science, and also mathematics, as a double agent, in which it operates and serves both the 'good', as for 'evil', depending on the interests given by the logic of the system.

This modus operandi can be observed in the context of wars. The link between the 'art of war' and mathematics is an ancient one. From a long time ago, mathematics began to figure as an important and useful element in the mechanics of war, a practical knowledge required in the field of military art. It is in practical necessity (that of military constructions and artillery) that mathematics has completely altered the meanings of defenses and attacks in wars (Valente, 1999). According to this author, the first firearms appeared in the 14th century and underwent rapid evolution/improvement, influencing the powers of defense and attack. After the significant transformation of use cannons, for example, new questions and problems about defenses emerged. So,

> The walls of medieval fortresses no longer resist the onslaught of cannon balls. More than ever, the "art of fortifying well" becomes a state business. Books on fortification are multiplying, engineers are transformed into great characters and fundamental figures of power (Valente, 1999, p. 41-42, our translation).

In this context, some areas of mathematics, such as arithmetic and geometry, ended up becoming guarantees of security, which are "used as an instrument of persuasion due to their ineffability and the new insights and fecundity that demonstration makes possible" (Vérin, 1993, apud Valente, 1999, p. 42, our translation). In this way, it is considering the knowledge of geometry that the practice of engineers is elevated and ends up being configured in fundamental roles for the combatants. Therefore, it was up

to geometry to become the support of military treaties and writings (Valente, 1999). Thus, if, on the one hand, mathematical knowledge, here in the specificity of geometry, allows the development of new fortification instruments, so that they are considered powerful technologies for war, on the other hand, we find an inhuman operationalization, arising from this knowledge and the technologies that emerge from it. In this scenario, there is one more clear example that the ideology of progress "does not simply bring 'wonders'. It is also accompanied by 'horrors'"(Skovsmose, 2007, p. 142, our translation).

To understand this "expansion" of mathematics as an instrument of war, let us look, for example, at its emergence and development in Brazil. As a european colony, initially, the country was concerned with its own formation, expansion and stabilization with the production of demographic and material wealth. The men who at the time were called mathematicians came to Brazil on missions and work on cartography, astronomy and engineering (Leite, 1945 apud Valente, 1999). As for school mathematics, its origins are rooted in the late 17th century, when, through the *Aula da Esfera do Colégio de Santo Antão*, students learned to introduce contents in geometry and arithmetic. Subsequently, in response to a royal determination of King João IV, the school started in the *Aula* a kind of preparatory course for students, whose destiny was to attend the *Aulas de Artilharia e Fortificação*, in which practical geometry, that of engineers, was considered as fundamental matter (Valente, 1999).

Founded in 1647, in Portugal, by D. João IV, the *Aula de Fortificação e Arquitetura Militar* had the important task of reorganizing its military force. At that time, "it was urgent to become aware of the advances made in the art of war. The expedient was to hire international experts on the subject. Such a practice was common among countries whose aim was to improve their armies" (Valente, 1999, p. 43, our translation). Thus, after Portugal, in 1648, "the Portuguese Court hired foreigners, specialists in military courses, to come to Brazil to teach and train qualified personnel to work with military fortifications" (Lyra Tavares, 1965 apud Valente, 1999, p. 43, our translation).

From the 18th century, Brazil was in the great rush for gold, which ended up moving an initial disorderly exploration, influencing the Portuguese Crown to take "successive measures to always collect as much as possible, [thus] physicists and military took command of the organization, foundation of villages and construction of civil life in regions created by mining" (Valente, 1999, p. 43, our translation). In this context, with the increase in exploited wealth, threats to the territory also increased, which, in turn, increased the need to defend itself. This was decisive in the creation of the School of Fortification and Military Architecture, which later split into two branches: military education and family education (Valente, 1999).

According to Valente (1999), the *Aula do Terço de Artilharia do* Rio de Janeiro represented the initial moment of the formation of an important class in colonial society. Through a course, which became the basis of military schooling, the children of soldiers and nobles could now pursue a war career at the *Aula de Artilharia e Fortificações do* Rio de Janeiro. Thus, we realized how the military schools were related to mathematics, not only for their theoretical knowledge, but also, strongly, for their practical knowledge, such as the geometry of engineers.

With this brief example about the constitution of mathematics in Brazil, we note that it was linked, in the initial moments, to the ideas of the art of war and the conquest of powers (social, political, territorial, economic, among others). So, given everything exposed here, can we really conclude that mathematics and its theoretical evolution are intrinsically linked to war? It is worth remembering, at this moment, the question that moves us to think about such a discussion, which is the intellectual arms race in which ciphers and deciphers acted and still act in the search for the power of secrecy (Singh, 2008). This race is due to mathematics and the power it exerts on encryption and decryption algorithms. In this way, the question raised above becomes even more complex in the sense that, nowadays, information and its secrecy are one of the most influential characterizations of power, be it social, political, territorial, economic, , etc.

In view of all this discussion, we see that mathematics and its generating conflicts are closely intertwined, the line that separates them being tenuous, and at times it can be considered and

operationalized as a potential knowledge of freedom and emancipation, and at times, under it, it can be conceived and used as uncomfortable and subordinate (Skovsmose, 2007). In this regard, D'Ambrosio (2011) argues that:

> We spent the year 2000 with great festivities, we were threatened by the millennium bug, the product of powerful viruses built with sophisticated computational mathematics, we escaped this bug thanks to powerful antiviruses developed thanks to the same mathematics, we went through the year 2001, which ended under the impact of the attacks terrorist attacks in the United States and retaliatory attacks in Afghanistan. All performed with mathematical precision. And now, in 2011, we witness local civil wars and international entanglements with unpredictable consequences. All based on the use of high technology, developed thanks to the extraordinary advancement of science (D'Ambrosio, 2011, p. 68, our translation).

In this context, Bauchspies and Restivo (2001, p. 2) mention the position of 'seeing' and 'feeling' mathematics as "something pure, transcendent and certain, with results that approach a level of veracity as high as human beings can hope to reach." That said, it is necessary to reflect that mathematics by itself, as a science that develops and organizes itself in formal structures, well defined and organized in its axioms and postulates, seems, at first glance, as pure, naive, accurate and need.

Such a view is supported by the perspective of the ideology of certainty (Borba & Skovsmose, 1997), in which the central idea rests on two facts: a) the purity and generality of mathematics and b) its role as a science that provides applications in different situations. As raised by Guimarães (2022), this ideology is present in discourses that permeate the teaching and learning processes, in addition to newspapers and scientific programs, in which phrases such as 'numbers express the truth' are taken as absolute truths about mathematical knowledge, masking any subjectivity inherent in 'doing math'.

However, the notion of "mathematics in action" discussed by Skovsmose (2007) also points out that to this same mathematics we can have operationalizations of different types and purposes, always mediated by the intentions and actions of those who hold it, representing a scenario of unpredictable mixtures in terms of to its wonders and horrors (D'Ambrosio, 2011; Skovsmose, 2007). It is in this scenario that D'Ambrosio (2011) raises questions about the possible irresponsibility of scientists or a passive naivety, and also raises the question about when mathematics ceases to be related to war and starts to be related to peace.

Upinsky (1989) also argues about the use of technologies for good or for evil. Let us take as an example of these technologies in cryptography the Enigma machine and the machine called bomb. During World War II, the Enigma machine was considered, according to Singh (2008), as being the most fearsome encryption system in history, used by the Germans and ensuring the transmission of messages between the Nazis in a secure and confidential way. However, it was another machine, the so-called bomb, developed by Alan Turing, that managed to decipher the Enigma in a powerful way, thus weakening communication between the Germans. At this point, we perceive the neutrality of technologies, as defended by Upinsky (1989), and their use is what characterizes them as being for 'good' or for 'evil'.

Upinsky (1989) also emphasizes the ideas of information transformation. According to him, this topology often misrepresents and reorganizes the different structures and spaces, such as financial, economic, social, political and cultural. Within this thought, the author observes that, with these changes in space, soon people will be increasingly connected to others, to environments, by means of numerals, formulas, increasingly complex, interactive and interconnected means of communication.

With the ideas presented by D'Ambrosio (2011) about the irresponsibility or naivety of scientists, and with the relationships of mutation and connection of space and people brought by Upinsky (1989), a careful reflection on technological advances is underway. According to Hobsbawn (1995), technology, based on advanced theories and scientific research, dominated the economic boom around the second half of the 20th century. According to him,

> The problem with these technologies is that they were based on discoveries and theories so far removed from the world of ordinary people, even in the most sophisticated developed countries, that only a few

> dozen or, at most, a few hundred people in the world could initially grasp that they had basic implications (Hobsbawn, 1995, p. 507, our translation).

In this regard, to contextualize his thinking, Hobsbawn (1995) argues that physics and mathematics already governed mills machine in the 17th century, and chemical and electrical discoveries and early 19th centuries already became essential to industries and communications. In this walk, we see how important the explorations of scientific researchers were and recognized as the essential start for technological advancement. As a conclusion of this observation, the author argues that technology, based on science, was at the heart of "the bourgeois world of the nineteenth century, although practical people did not know exactly what to do with the triumphs of scientific theory, unless, in appropriate, transform them into ideologies" (Hobsbawn, 1995, p. 507, our translation). Looking at the history of cryptography, technologies appear around the 15th century, with the cipher disk, invented by Leon Alberti, but it was only in 1918 that the mechanization of these gains strength, with the creation of Scherbius, the Enigma machine (Singh, 2008).

To exemplify how these advances occurred, Hobsbawn (1995) cites two important figures in the history of humanity: Otto Hahn and Alan Turing. The first, a German physicist, discovered nuclear fission in early 1939. The second provided an important work for the history of computing. Turing, who initially worked with speculative exploration for mathematical logics, eventually developed the basis of modern computational theory (Hobsbawn, 1995; Singh, 2008). However, as Hobsbawn (1995, p. 508, our translation) states, "the war gave him, and others, the opportunity to translate theory into the beginnings of a practice for deciphering codes, but when it was published no one, with the exception of a few mathematicians did not even read it", or wanted to know about this work.

It is at this threshold that the sciences were encouraged, supported and finally used. Based on this, despite the fact that this type of scientific investment resulted in catastrophes such as the attack on Hiroshima, the 20th century was marked as the century of human growth. This shows the way in which the structures of research and scientific theory have arisen (Hobsbawn, 1995). Upinsky (1989) describes a quote from Albert Speer (1905-1981), who argues about the relationship between communication techniques and the initiative of totalitarianism during the Second World War. According to Spier,

> Thanks to technical means such as radio and loudspeakers, eighty million men became slaves to the will of a single individual; [and concluding that] the telephone, telex and radio enabled the highest authorities to immediately transmit their orders to the lowest echelons who applied, without question, the reasons of the high authority from which they came... These means made possible an extreme ramified surveillance of citizens, at the same time the possibility that criminal actions remained secret (...) (Speer, 1971 apud Upinsky, 1989, p. 171, our translation).

By referring to the history of cryptography evolution, it is clear how the development and use of these means of communication during the Second World War took shape and influenced the situations of battles and information transmissions (Singh, 2008). Technological advances and changes are linked to strong political and financial interests, as already mentioned. Therefore, we can raise the question that the future of the next wars will emerge on the internet and, according to Tamdjian and Mendes (2010), many countries are already aware and preparing to face these types of problems. According to these authors,

> This situation of digital disputes is showing that conflicts can occur between countries or groups of countries, blocking or sabotaging rival computer networks as a way of making the opponent vulnerable, causing his/her paralysis and leading to chaos, since The use of computers around the world is increasing day by day, and their relationships with economies are increasingly deeper (Tamdjian & Mendes, 2010, p. 44, our translation).

At this moment, in the same way that we seek to understand a history through the lens of the relations between power and mathematics, in the specificity of cryptography, we become aware of the present, in the direction of realizing how delicate it is to deal with technological developments and how much their practical applications are. can result in lifesaving (wonders) or catastrophic (horrors) situations.

The dichotomy today: what is the nature of this responsibility

With advances in information technology, it is possible to observe situations that allow people to work from virtually anywhere. With the progressively unlimited transmission of data, the expansion of connectivity has been "significantly altering society and large business corporations" (Tamdjian & Mendes, 2010, p. 36, our translation). In this scenario, it is possible to observe how the internet is linked to these technological innovations.

However, paralleling this growth, there are also developments in data security. Ensuring consumers, companies and governments exchange sensitive data is as important as the efficiency of the internet itself. It is in these aspects that the initial ideas in the discussion proposed in this text are resumed: the importance of secure ciphers to ensure data transfer continues to evolve, as decryptors continue to search for breaches, thus obtaining the secrets. At the same time, a "permanent reconfiguration of old knowledge in new studies promotes unpredictable leaps" (Skovsmose, 2007, p. 158, our translation).

As an example of secure encryption, we can cite RSA, which is considered the most influential cipher system in modern cryptography. Discovered in 1977 by two computer scientists and a mathematician, RSA is based on the results of number theory regarding the modular function and constitutes an asymmetrical system also known as *public key cryptography*. Its efficiency in terms of information security is structured on the identification of large prime numbers and on the difficulty of factoring a number into two prime numbers, when it is extremely large (Singh, 2008). Because of its power to keep information confidential, RSA continues to be used today.

That said, in view of everything discussed here, we realize how mathematics, the need for security, information and technological advances are intertwined with power disputes and, consequently, with the powers constituted by them. The types of crimes that occur in cyberspace have drawn the attention of large countries, generating huge investments in new technologies. To exemplify this situation, Tamdjian and Mendes (2010) present a moment of concern for the US authorities, in which

> the government created a Digital Military Command to protect the government and Armed Forces computer network from intrusion. Matters that seem like science fiction today will soon become reality. An example is the news that digital spies have installed programs on computer networks in the United States that can interrupt the functioning of millions of computers, leading to the paralysis of the economy and many activities and, consequently, causing incalculable losses (Tamdjian & Mendes, 2010, p. 43, our translation).

Corroborating these concerns, Upinsky (1989) reflects on the large amount of information that cyberspace contemplates and how its handling can affect society:

> The fantastic volume of banking, economic, political and social information that travels through space via satellites, radios, cables, etc., [is] dizzying; a simple bank entry (just a few "digits") crosses space and as a result a factory closes and families are thrown into misery. The dollar drops on the New York Stock Exchange and immediately follows a multitude of events directly affecting the lives of millions of people (Upinsky, 1989, p. 175, our translation).

However, care must be taken in raising these questions regarding the importance of secrecy and the extent to which it influences nations. We agree that fights between ciphers and deciphers exist and that they are increasingly based on mathematical theories. However, it is highlighted here that the actions of encryption and decryption do not assume fixed characteristics, being "good" or "evil". Deciphering the Enigma machine's secrecy during World War II, for example, was an important factor in contributing to the oppression of the Nazis' expansion. However, breaking the secrecy of people's bank details is a breach and therefore a digital crime.

It is in this reflection, on the acts of keeping or not the secrecy of information, that we present an important case that is currently in circulation. The possible internet war highlighted by Tamdjian and Mendes (2010) may have started in 2010, when a website called Wikileaks began to release secret US files on the War in Afghanistan and the War in Iraq, containing many serious allegations against respect for human rights violations. Wikileaks is a transnational, non-profit organization that publishes data

from anonymous sources on its website, revealing documents, photos and confidential information, leaked from governments or companies. Its editor and spokesman, journalist and cyber activist Julian Assange, was, since 2012, in political asylum at the Ecuadorian embassy in London. In 2019 he was arrested and remains to this day in Belmarsh Prison in London. His extradition to the US is still on trial and Assange continues to fight with the UN for the right to freedom and compensation.

While for some countries the leak of information generates great conflicts, for others the initiative to reveal hidden truths is characterized as one of the most important doors of transparency and freedom of expression. This sets a precedent for the dissemination of information on corruption, human rights violations and war crimes. As a result, the site was even nominated by the Norwegian parliament in 2011 to compete for the Nobel Peace Prize.

It is with this situation and with everything that has been discussed in this text that we observe and reflect on how cryptography and cryptanalysis have, for a long time, been gaining ground in the history of humanity and configuring themselves as elements of power. Linked to wars in their constant intellectual arms races, and to mathematics with its theoretical-technological advances, it is possible to perceive the complexity of this subject and emphasize the importance of initiating discussions about the powers of information and secrecy, in elementary school.

Weaving some reflections: perspectives on student education

To what extent does bringing cryptography as a didactic element for the teaching of mathematical concepts reflect on its role in the context of wars and power disputes? How to bring elements of reality to contribute to the meanings of mathematics without reinforcing a power discourse that promotes more inequalities, misinformation and catastrophes? We understand in these questions some directions for reflection, which need to be at the heart of pedagogical practices in mathematics, in the student education, especially with a critical eye (Skovsmose, 2007) and the search for peace (D'Ambrosio, 2011).

As presented by Valente (1999), history shows the impact of this science on the education that was offered to students, based on the bias of applying knowledge as a means for the production of artillery and fortifications. Currently, we identify that cryptography has been present in Brazilian textbooks, as a way to bring mathematical concepts. However, we observed that his approach still only surrounds the algorithmic and procedural ideas regarding the objective of encrypting/decrypting messages in order to present and/or develop such concepts. The articulations between mathematics and the fields, for example, History and Sociology, when they are carried out, occur with very brief passages, failing to provide opportunities for reflections on the role of cryptography in contemporary society, that of information security and the interrelationships between the power, mathematics and cryptography (Litoldo & Guimarães, in press; Litoldo & Lazari, 2014).

The discussions raised by Bauchpies and Restivo (2001) and Borba and Skovsmose (1997), for example, can be enriched during the teaching and learning processes precisely in this reflection on the role of mathematics in student education, in the sense that cryptography, being related to other areas of knowledge, it promotes a challenge to the ideology of certainty (Guimarães, 2022) and the supposed neutrality of mathematics. Thus, this can be another path that helps the teacher to think about an education focused on criticality and peace, aiming to achieve a 'good' role for the use of mathematical knowledge, in particular, cryptography.

Therefore, we emphasize the importance of paying attention to the discussions proposed, for example, in this text, as a way to promote reflections on the future horizon, since we understand that the path of these interrelationships is on uncertain terrain and, still, traveling a bias of the ideology of progress.

References

Bauchspies, W. K., & Restivo, S. (2001). O arbítrio da matemática: mentes, moral e números. *Bolema-Boletim de Educação Matemática*, *14*(16), 102-124.

Borba, M. C, & Skovsmose, O. (1997). The ideology of certainty in mathematics education. *For the learning of Mathematics*, *17*(3), 17-23.

D'Ambrosio, U. (1994). Cultural Framing of Mathematics Teaching and Learning. In R. Biehler, R. W. Scholz, R. Sträßer, & B. Winkelmann (Orgs.), *Didactics of Mathematics as a Scientific Discipline* (p. 443-455). Kluwer Academic Publishers.

D'Ambrosio, U. (2011). A busca da paz: Responsabilidade de matemáticos, cientistas e engenheiros. *Revista da Universidade Vale do Rio Verde, 9*, 66-77.

Guimarães, D. R. (2022). *Educação matemática crítica permeando capítulos de geometria em livros didáticos: entre direcionamentos, contextos e enunciados*. Mestrado em Educação Matemática. Universidade Estadual Paulista.

Hobsbawn, E. J. (1995). Feiticeiros e aprendizes: As ciências naturais. In M. Santarrita (Trad.), *Era dos extremos: O breve século XX* (p. 504-536). Companhia das Letras.

Litoldo, B. F. (2016). *As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim* Masters dissertation in Mathematics Education. São Paulo State University.

Litoldo, B. F., & Guimarães, D. R. (no prelo). Criptografia e Livros Didáticos do Ensino Médio: Uma análise sobre as novas obras didáticas específicas do PNLD 2021. *Abakós*.

Litoldo, B. F., & Lazari, H. (2014). Uma análise do uso da criptografia nos livros didáticos de Matemática do Ensino Médio. *REMATEC*, *17*, 133-152.

Skovsmose, O. (2007) *Educação crítica: incerteza, matemática, responsabilidade*. (M. A. V. Bicudo, Trad.). São Paulo: Cortez, 304 p.

Singh, S. (2008). *O livro dos códigos: A ciência do sigilo do antigo Egito à criptografia quântica*. Record.

Tamdjian, J. O., & Mendes, I. L. (2010). A construção das novas geografias: A internet, o espaço a Antártida. Em *Geografia: Estudos para a compreensão do espaço* (1º, Vol. 3, p. 34-56). FTD.

Upinsky, A. A. (1989). *A perversão matemática* (A. R. de Oliveira, Trad.). Francisco Alves.

Valente, W. R. (1999). *Uma história da matemática escolar no Brasil (1730-1930)* (1º). ANNABLUME.