2. Introducing New Content into a School Mathematics Curriculum: The Case of Cryptology

Kalvin Whittles, Ole-Einar Torkildsen,
Cyril Julie and Trygve Breiteig

Few false ideas have more firmly gripped the minds of so many intelligent men than the one that, if they just tried, they could invent a cipher that no one could break. (Kahn, 1996: 763)

Concealment, codes, and other types of ingenious communication. (Butler and Keeney, 2001)

Abstract

Developing learning resources forms an important part of a school mathematics curriculum implementation. This chapter argues for a change in the way we do analysis for developing learning resources. An argument is forwarded for an understanding of the main concepts within the topic as well as a historical and didactical analysis thereof in order to make statements with respect to the teaching and learning of the topic. For this analysis, the topic of cryptology is used as an example. The chapter concludes with recommendations to curriculum designers to revisit the accepted practice to adapt already historically and didactically analysed materials, and warns on the consequences of the currently used methods.

Introduction

The development of instructional materials is an important aspect of curriculum development. It becomes even more important when new content is introduced into a school mathematics curriculum. The current practice in South Africa is to have workshops where the curriculum advisers for school mathematics give in-service training on the content of the new curriculum to teachers of school mathematics. No training with respect to material development is given and an example is usually given as an activity to explore a section of the topic under discussion.

This chapter argues for a historical and didactical analysis of the topic under discussion, as well as a conceptualisation thereof. The topic chosen for this purpose is cryptology. Cryptology refers to 'cryptography, cryptanalysis, and the interaction between them' (Barr, 2002: 2).

The first part of the chapter scrutinises the topic of cryptology. This section aims to explain cryptology as a cryptosystem. In order to understand this cryptosystem, it is important to have a sense of where the overall concepts, discussed in the cryptosystem, fit in. This is followed by an elaboration of the different concepts important to cryptology and their relationship with a cryptosystem. The highlighting of the important concepts within cryptology is done so as to inform the discussion on the historical and didactical phenomenology later on. The section concludes with a figure to outline the cryptosystem and to position the important concepts in the cryptosystem.

The second part of the chapter presents a historical and didactical phenomenological analysis of cryptology. An important aspect neglected when developing new curricula is the link between the historical developments of the knowledge constructs embedded in the subject matter. The consideration of the historical development of knowledge constructs might (or might not) point towards different learning possibilities for the topic under scrutiny.

Cryptology

The word 'cryptology' has it origins in ancient Greek. Cryptology is derived from kryptos, meaning hidden, and logos, meaning word. The field of cryptology has two divisions, namely cryptography and cryptanalysis. So whenever the word cryptology is used in the text, it refers to cryptography, cryptanalysis and the interaction between them (Barr, 2002: 2). Cryptology is also known as the study of codes.

Over the years, people have used secret messages. The need for secret communication has occurred especially in diplomatic, military and financial affairs. With the increase in electronic communication, it has become essential to safeguard such communication by introducing secrecy measures. There is thus a great deal of interest in the ways of making the transmission of messages of a sensitive nature to a next person or institution more secure.

Cryptography

The aim of cryptography is to allow two parties A and B to communicate in such a way that C – a listener, intruder or opponent – is not able to understand what is being said. Cryptography is also seen as a discipline to keep communications private (Barr, 2002; Stinson, 1995; Beutelspacher, 1994). In order to keep the communication private, it is obvious that it cannot be conveyed in the same or understandable text that is commonly used. Nor should these private communicative texts be such that they are easily analysable by a third party. In cryptography the easily understood and commonly used text is referred to as the 'plaintext'. The secret text is known as the ciphertext. The word 'cipher' comes from the Hebrew word 'sapher', which means number. The objective of cryptography is the conversion of plaintext to ciphertext, and vice-versa. Ciphers can be seen as mere substitutions in that a letter of the alphabet is substituted by another letter – it could be by one letter, two, or more. A code, on the other hand, is an algorithm, key or a rule for changing a legible message into an intelligible form. In order to change an intelligible message into readable form, one has to use some sort of codebook for these changes.

The process of changing the legible text, also called the plaintext, into an intelligible form is called enciphering or encoding. The reverse process – that is, changing the intelligible text (also called the ciphertext) into plaintext – is called deciphering or decoding.

Menezes, Van Oorchot and Vanstone (1997) go a step further and define cryptography as: 'the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.' For a message to be hidden from prying eyes, a key or algorithm is used to make it secure. This key or algorithm takes on different forms. Historical examples of keys used in sending messages include battens (scytales), linear equations and shifting

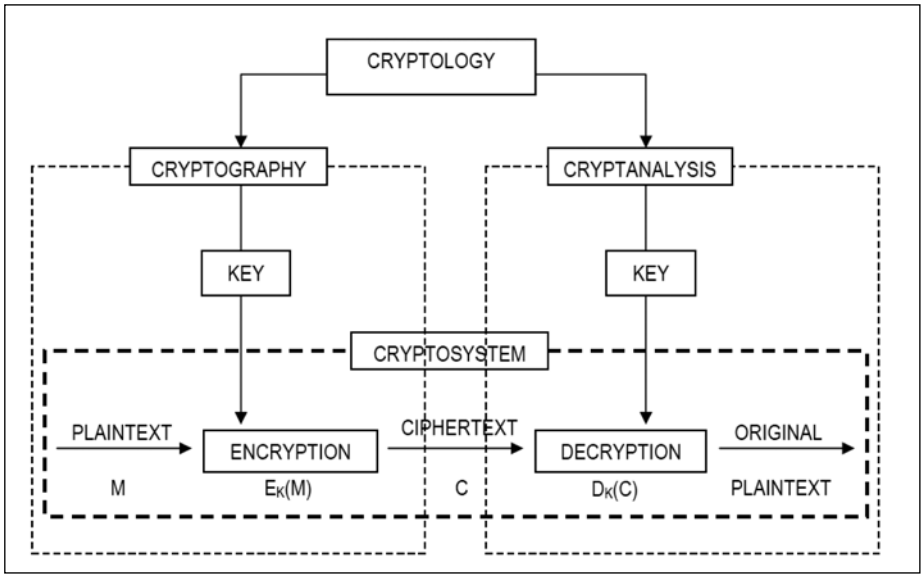
of letters. The importance of keeping the key secret is summarised by the Kerchoffs Principle, paraphrased in Singh (1999: 12) as follows:

> Don't underestimate the enemy. The idea is not to keep the encryption and decryption algorithm secret. The main idea is to keep the key itself secret.

Cryptanalysis

Cryptanalysis is the process of converting a received message from ciphertext into plaintext. The person involved with breaking the ciphertext (secret message) is called a cryptanalyst. Based on the discussion above, the Figure 1 gives a summary of how cryptolology is seen as a cryptosystem.

Figure 1: Diagrammatic representation of cryptology and its components



Phenomenology

Phenomenology can be described as an objective inquiry into the logic of essences and meanings of trying to make sense of a topic. This objective enquiry can take on different forms. Possible forms are a theory of abstraction, deep psychological description, or an analysis of consciousness (Thévenaz, 1962: 37). Phenomenological analysis means approaching the study object, the phenomenon, as free as possible from

conceptual presuppositions. The aim of phenomenological research is to obtain insights into the essential structures of these phenomena on the basis of mental examples supplied by experience or imagination and by a systematic variation of these examples in the imagination.

Freudenthal (1983a), however, goes a step further by describing a method for studying relations between mathematics, history and education. He distinguishes between *phenomena* and *concepts*. Phenomena refer to that which we want to understand, make sense of, or structure; while concepts are the thought processes which organise these phenomena. Based on this, Freudenthal (1983a: 28–29) defines phenomenology as follows:

> Phenomenology of a mathematical concept, a mathematical structure, or a mathematical idea means, in my terminology, describing this nooumena in its relation to the phainomena of which it is the means of organizing, indicating which phenomena it is created to organize, and to which it can be extended, how it acts upon these phenomena as a means of organizing, and with what power over these phenomena it endows us. If in this relation of nooumenon and phainomenon I stress the didactical element, that is, if I pay attention to how the relation is acquired in a learning-teaching process, I speak of didactical phenomenology of this nooumenon. (…) if 'is … in a learning-teaching process' is replaced by 'was … in history', it is historical phenomenology.

Within the context of this chapter, historical phenomenology and didactical phenomenology have to be clarified. Historical phenomenology is the study or probing of historical contexts wherein certain mathematical concepts are present in order to make sense of why and how they came up in these contexts. Didactical phenomenology, on the other hand, is the study of relationships 'between the mathematical concepts and the phenomena in which they arise with respect to the process of teaching and learning these concepts and their applications' (Bakker, 2003).

This brings us to one of the aims of this chapter: to make a study of cryptology from two stances, i.e. from a historical and didactical stance. What now follows is a historical phenomenology of cryptology. The chosen examples are organised chronologically and are by no means exhaustive.

Historical and didactical phenomenology of cryptology

According to Freudenthal (1973; 1991) learners should be given the opportunity to re-invent, in a guided way, the concepts and ideas in a particular mathematical domain. He states:

> The young learner recapitulates the learning process of mankind, though in a modified way. He repeats history not as it actually happened but as it would have happened if people in the past would have known something like what we do know now. It is revised and improved version of the historical learning process that young learners recapitulate. 'Ought to recapitulate' – we should say. In fact we have not understood the past well enough to give them this chance to recapitulate it. (Freudenthal, 1983b: 1696)

From this it is clear that Freudenthal, and by implication the Realistic Mathematics Education movement, views it as important that development work in the domain of mathematics for school teaching and learning should take into account the historical development of the domain. The purpose of this consideration is to ascertain whether learning trajectories which emulate the historical unfolding of the domain can be determined. A consideration of this nature is called a historical phenomenology, and Bakker (2000) describes it as follows:

> Exploring the literature on cryptology gave some insights into the links between history and education and opens up avenues for different learning trajectories for cryptology. On developing these learning trajectories, the aim is that learners somehow reinvent, in a guided way, the mathematical concepts …

In order to make sense of or understand concepts within a mathematical topic, it is useful to look at its history. Freudenthal (1983b) and Stanton (2001) support the notion that studying the history of a topic is good for teaching that topic. Such examination is aimed at determining what motivated its emergence and shaped its development. Dijksterhuis (1990) is of the opinion that the historical analysis of a topic allows learners to have a better understanding of the topic under discussion. Problems that current learners of school mathematics encounter resemble problems that generations before them experienced. With this in mind, I will look for

historical contexts that open up avenues for cryptological notions and conceptual obstacles that mathematicians and users of mathematics encounter.

A historical study of secret messages is not an easy process. When people write about history, it is usually with respect to people or events, and rarely with respect to concepts. A second problem could be that the topic of secret messages is not an established one that stands on its own in mathematics. The historical phenomenology of secret messages will therefore look at examples within the different contexts in which it was used. Therefore, what follows is instead an exposition of how secret messages were used in war, communication and other contexts. There are also senses of enciphering and deciphering, so it is not strictly 'use' only but also the processes of 'making secret on the one hand and unmaking the secret on the other hand' – this is the crux of the matter in the historical phenomenology.

Bald messages

Herodotus (Singh, 1999) in 'The Histories' chronicled one of the earliest conveyances of a secret message. It is related how Histaiaeus, governor of Miletus, and an enemy of the Persian ruler, Darius, secretly communicated with Aristagoras. Histaiaeus shaved off the hair on his messenger's head and tattooed a message on his scalp. After a few weeks, the hair on the messenger's head grew back on, covering the message. The messenger was sent to Aristagoras to deliver the message. He had no problems in crossing Persian enemy lines. On arrival before Aristagoras he said: 'Master, shave my head.' This was done and the secret message revealed. Covering of the message was ensured by the hair that grew back on the head.

For the bald message approach, both the enciphering and deciphering keys are shaving of the hair. As the original message remained the same (as inscribed on the head), there were no changes in the plaintext message. The bald message is an example of a plain cipher, as the message did not undergo any changes. The person carrying the message serves as the code as well.

A belt

Another instance in antiquity of relaying a message secretively is provided by Lysander (Laffin, 1964). He relates how a Spartan general and his troops were away from home, Greece, for quite a while. Their allies in the

war, Persia, remained behind to safeguard Greece against their common enemies. One day a messenger arrived at the war front and was brought before Lysander. On asking the messenger what his business was, he could not say. Lysander then saw the broad leather belt around the messenger's waist. Under scrutiny, Lysander found different letters branded into the belt. He took the belt and wrapped it around the long wooden baton he carried with him. In so doing, the scrambled letters aligned into legible words and sentences. The message thus uncovered informed him of a possible uprising in Greece by Pharnabazus from Persia. Wrapping the belt around the baton uncovered the message. Covering the message was ensured by wrapping it around something thicker – the waist of the messenger.

The wooden baton in this method of constructing and deconstructing a secret message acts both as enciphering as well as deciphering key. Turning the belt around the wooden baton also extended the keys to include a certain number of turns for both instances. An outcome of the turns was that the original message was scrambled on the belt after it was unwound from the baton. This is an example of a transposition cipher, meaning the ciphertext contained the same letters as in the plaintext, but in different positions.

Fire signals

Aeschylus, a dramatist, related the story that the fall of Troy (Butler and Keeney, 2001) in 1084BC was news so important that it had to be relayed to Queen Clytemnesta in Argos. The problem was that she was about 805 kilometres away.

Before the Queen left for Argos, it was agreed upon that a visible fire would indicate a good outcome. The Greeks arranged for fires to be lit on nine hills each about 72 kilometres apart. Different fire teams gathered on the respective hills, and on noticing the fire 72 kilometres back, lit their own to notify the next fire team. This, being the first recorded use of long-range communication, took about 11 minutes to travel the length of Greece.

Flag signals

During the 1800s, fleets of ships communicated with each other by way of flags. This innovative way of communication was used by the British by hoisting flags whose designs, lines, shapes and colours each had their own specific meaning.

In the Battle of Trafalgar (1805) between the British and French forces, use of a new signal system proved decisive in Britain winning the war. After much consultation with his flag lieutenant, the following message was sent by Admiral Horatio Nelson using seven flags: *'England expects that every man will do his duty'* (Butler and Keeney, 2001: 38). The message inspired the British to a victory over the French troops.

Quilt code

The quilt code was developed by slaves in America to indicate escape routes to Canada. According to Tobin and Dobard (1998), the different designs each conveyed a different instruction. Although the slaves could follow the instructions given on these quilts (generally hung on washing lines), outsiders and even slave owners could not make sense of them.

Hobo messages

As the economic depression increased in the 1930s, more and more people lost their jobs and became wanderers. In their wanderings, they often used signs, marks and symbols on sidewalks, houses, towns and cities to communicate different meanings. Only hobos understood this secret language of symbols.

Sports codes

Signs by way of number calls, hands and fingers are a prominent feature of various sorts of games. Any game on a baseball field is rife with hand signals. Rugby players also use numbers to indicate a code for finding a lineout jumper when throwing in a ball at a line-out.

For the fire, flag, quilt, hobo and sport messages substitution ciphers are included. They all have in common the fact that symbols in whatever form have been used to indicate different things. For example, the fire was a symbol of good news, whereas the designs on the flag denoted different words. In the case of the quilts and hobo messages, patterns and markings translated a language only to be understood by the people concerned. Concerning the sports codes, these signs and signals are there to indicate the play that is about to take place, and is aimed at keeping the opposition guessing.

For the examples listed under substitution ciphers. the symbols, patterns, fires, etc. indicate the encryption keys, while the decryption key was the translation of these into a plain message or an action.

Pig Latin

Pig Latin was developed by children as a way to keep their communication secret or confidential and has been in use since the 15th Century, according to Kahn (1996). If two children communicated, they used Pig Latin to keep their communication secret from a third party. The Pig Latin system works as follows:

- Words that start with a vowel (A, E, I, O, U) have 'way' appended to the end of the word.
- Words that start with a consonant have all consonant letters up to the first vowel moved to the end of the word and 'ay' appended at the end.
- 'Y' is counted as a vowel in this context.

The sentence *'Please pass me the yellow spoon'* changes to *'Easeplay asspay emay ethay elloyay oonspay'* in Pig Latin.

Pig Latin is a simple form of a transposition cipher where letters in a word change positions. The adding of the *'ay'* or *'way'* at the end are examples of a null cipher. A null cipher is an example of a cipher that does not change a word or its form. This is one of first examples in history where two ciphers were used.

The above examples can be viewed as 'proto-cryptography', since, in Freudenthal's terms, they are yet not 'organised', but from a phenomenological perspective they provide possible entry points for the topic.

Conclusion

The examples listed above show how difficult it is to make implicit aspects of cryptology explicit. Although Lysander thought of the shaving of hair to inscribe a message on the head and later allowing the hair to grow back to cover the same message as a way of keeping it secret, this will not be a good example to use for teaching. Both the encoding and decoding keys are the same and the message itself did not undergo any changes.

The observation that the oldest historical examples had to do with secrecy, gives rise to the question: *'Is secrecy a good starting point for the teaching and learning of cryptology?'* The answer is yes. Cryptology has secrecy or confidentiality as its aim. The historical examples show the messages had elements important to cryptology. Some of these elements are the encoding key, decoding key and the different types of ciphers.

Another observation from history is that the idea was to keep messages/communication secret. This alludes to the importance of the key/rule in encoding messages. The more difficult the key/rule, the more difficult it will be to decode the message.

For the teaching and learning of cryptology, the historical examples need changes or revision. Firstly, most learners have their own understanding of what secrecy is and use it, unwittingly, in different situations; for example, in communication when using Pig Latin in situations of play. Secondly, not all the historical contexts are suitable for instruction. How many learners would be interested in deciphering flag signals or hobo messages? The example of the belt, however, is an appealing context to start the teaching of cryptology. It has elements of a practical activity as well as introducing a transposition cipher.

The examples of history serve to introduce different ways of communication to keep messages secret. In all these messages the way of hiding the message – namely, the key – was a central concept. For the teaching and learning of cryptology it seems it would be best to introduce the topic of cryptology by way of secrecy, and furthermore to introduce learners to the different ciphers in order to render messages intelligible.

This chapter set out to show how the concepts important to cryptology started back in history. Although only a few of these concepts were discussed, it shows the importance of the conducting of historical phenomenology for the designing of instruction material. This opens up ways for designers of curricula to explore the links between history and education. This could lead to a better understanding of the topic under discussion and give a bigger picture of the topic to be covered.

References

Bakker, A. (2000). Historical and didactical phenomenology of average values. In Radelet-de Grave, P. (Ed.), *Proceedings of the Conference on the History and Epistemology in Mathematical Education*, Vol. 1 (pp. 91–106). Louvain-la-Neuve, Belgium: Université Catholique de Louvain.

Bakker, A. (2003). The Early History of Average Values and Implications for Education. *Journal of Statistics Education*, 11(1), 17–26.

Barr, T.H. (2002). *Invitation to Cryptology*. Upper Saddle River, NJ: Prentice Hall.

Beutelspacher, A. (1994). *Cryptology*. Washington, DC: Mathematical Association of America.

Butler, W. and Keeney, L.D. (2001). *Secret Messages*. London: Simon and Schuster.

Dijksterhuis, E.J. (1990). *Clio's Stiefkind*. Amsterdam: Bert Bakker.

Freudenthal, H. (1973). *Mathematics as an Educational Task*. Dordrecht: Reidel.

Freudenthal, H. (1983a). *Didactical Phenomenology of Mathematical Structures*. Dordrecht: Reidel.

Freudenthal, H. (1983b). The implicit philosophy of mathematics: History and education. In Ciesielski, Z. and Olech, C. (Eds), *Proceedings of the International Congress of Mathematicians* (pp. 1695–1709). Warsaw and Amsterdam: Polish Scientific Publishers and Elsevier Science Publishers.

Freudenthal, H. (1991). *Revisiting Mathematics Education*. Dordrecht: Kluwer Academic Publishers.

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner.

Laffin, J. (1964). *Codes and Ciphers*. New York: Abelard-Schuman.

Menezes, A., Van Oorchot, P. and Vanstone, S. (1997). *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press.

Singh, S. (1999). *The Code Book*. New York: Anchor Books.

Stanton, J.M. (2001). Galton, Pearson, and the Peas: A Brief History of Linear Regression for Statistics Instructors. *Journal of Statistics Education* 9(3). [Online] www.amstat.org/publications/jse/v9n3/stanton.html [Accessed 16 April 2004].

Stinson, D.R. (1995). *Cryptography: Theory and Practice*. Boca Raton, FL: CRC Press.

Thévenaz, P. (1962). In Edie, J.M. (Ed. and Transl.), *What is Phenomenology? and Other Essays*. London: Merlin Press.

Thévenaz, P. (1962). *What is Phenomenology? and Other Essays* (Translated by Edie, J.M., Courtney, C. and Brockelman, P.). Chicago: Quadrangle.

Tobin, J. and Dobard, R. (1998). *Hidden in Plain View: The Secret Story of Quilts and the Underground Railroad*. New York: Doubleday.