

Bringing Cryptology into the Secondary Education Classroom

Catherine Murphy

University of Portsmouth
Winston Churchill Avenue
Portsmouth
PO1 2UP
catherine.murphy@port.ac.uk

Aaron Wootton

University of Portland
5000 N. Willamette Blvd
Portland, OR 97203
USA
wootton@up.edu

Abstract

Cryptology is becoming increasingly commonplace in undergraduate mathematics curricula as a way to motivate abstract mathematics. However, it is still typically absent in secondary education (students aged 11 to 18). In the following, we discuss why we think it would be advantageous to bring cryptology, both historical and modern, to the secondary education classroom. Additionally, we discuss some of the barriers we perceive to doing so and suggest, in our opinion, how they might be overcome. We illustrate implementation with a specific example of a topic in cryptology that could be included in a secondary education classroom.

1 Introduction

How does one motivate a group of recalcitrant teenagers to learn abstract mathematics on a wet Friday afternoon in January? Students need a ‘hook’, something that will engage and challenge their thinking. A concept that is relevant both to their lives and to their future careers.

In our experience, mathematics is viewed by some students as dry and boring, a subject with little real-life relevance and one which must be endured rather than enjoyed. However, it is fundamental to most (if not all) adults in the modern world. Without a grasp of mathematical systems, we would find ourselves unable to navigate the vista of technological advancement we find ourselves facing.

With its rich history and modern utility, we believe cryptology is an ideal vehicle for engaging students in complex mathematical problems. It is already used, with increasing regularity, in the undergraduate curriculum. There have been attempts to mimic this in secondary education,

(Caballero-Gil & Bruno-Castaneda, 2006), and evidence suggests its use improves student perception of mathematics and assessed performance (Özdemir, Güler & Aydın, 2011). Additionally, both authors have experience using cryptology to engage mathematics students, including the topic described below, and are convinced of its efficacy.

Unfortunately, the idea of using cryptology in secondary education has gained limited traction. So, what are the underlying issues and how can they be overcome?

2 Cryptology and mathematics

The overarching idea and practice of cryptology can be understood by suppressing the technical details in a black box process. Specifically, cryptology is about securely sharing information, for example, military strategy or financial data. A process, illustrated by the black box in Figure 1, is used to translate this information into an unintelligible piece of text, or ciphertext, which is then transmitted. Intended recipients have the tools necessary to recover the original information, but anyone else who intercepts the communication does not (at least in principle).



Figure 1: Black Box Process

It is in this black box that cryptology and mathematics are intertwined. Every cryptosystem, from the Caesar wheel to the RSA algorithm, can be described and analysed using mathematical principles. For example, the classical Caesar cipher, which translates the Roman alphabet forward by three letters, can be described using modular arith-

metic. Specifically, we assign both plaintext and ciphertext letters “A” to “Z” to the numbers 0 to 25 respectively. To encipher a plaintext letter, we add 3 to the number corresponding to that letter with the convention if the result is 26 or larger, we subtract 26 creating a wrap around, see Figure 2. An alternate correspondence often used in classrooms is to assign “A” to “Z” to the numbers 1 to 26, their position in the alphabet, (Lewand, 2004), with the mechanics of encryption being the same.

Figure 2: Caesar Cipher and Modular Arithmetic

3 Cryptology as a tool to motivate mathematics

and Mission Impossible films still holding box-office thrall. Furthermore, ‘escape rooms,’ which utilise encryption strategies, have become a pastime of the youth. In a nutshell, cryptology is sexy, and the considerable historical and political importance of cryptology gives it a frisson of excitement. So while some aspects of mathematics can appear dry, or indeed to have little purpose other than the mathematics itself, embedding the mathematics in a cryptological puzzle helps students to, not only see purpose, but also engage them in the mathematics.

ing (Stott, 2013), there are nonetheless aspects of this (progression and storytelling) that are naturally present. By approaching a concept in mathematics as a challenge, a puzzle to solve, students are likely to become engaged in their own learning, thus neatly sidestepping the problem of the recalcitrant teenagers attempting to study abstract mathematics on a wet Friday afternoon in January.

4 Barriers to cryptology in secondary education and how can they be overcome

There are many convincing arguments for incorporating cryptology into secondary mathematics education when viewed through the lens of mathematics educators. However, in our opinion, there are also significant barriers to doing so. The following we consider to be the most noteworthy.

The confidence (and qualifications) of some mathematics teaching staff may be an underlying issue. A report by the United Kingdom (UK) Government in 2023 on the school workforce in England showed that 12.8 percent of the total hours of mathematics taught in the secondary classroom was by teachers without suitable degree-level qualifications. Additionally, mathematics was one of the three subjects with the highest number of vacant teaching positions in the UK (Department for Education, 2023). This situation is not unique to the UK; a brief look at the mathematics teaching jobs available globally tells the sad story of the lack of mathematics teachers around the world. While the lack of suitable degree-level qualifications does not preclude teachers from being highly competent mathematicians, it is more likely that some may lack confidence and content knowledge. As a result, it may be less likely that a teacher will stray from a traditional mathematics course as set out by publishers, schools, and colleges.

Additionally, much of the underlying mathematics behind cryptology is not covered in the secondary education curriculum. This means students do not have the preparatory material to understand many cryptosystems. In addition, teachers without suitable degree-level qualifications may not have had exposure to this type of mathematics.

Another barrier is the pressure teachers feel to ‘teach to an exam’. Measures such as PISA and other international comparisons, as well as school and area-level comparisons and league ta-

bles within countries, look simply at results and do not consider the journey to knowledge. Teachers are often so anxious about their requirement to perform that there is little space left for autonomy (Ball, 2003). The idea of teaching a mathematical concept through cryptology may be perceived as inefficient and untried and, therefore, too risky to contemplate.

How can these barriers be overcome? In our opinion, they may, in part, be overcome through the creation of carefully curated resources that educators can utilise in their classrooms. These resources should be available to secondary education students and educators. Additionally, we believe it is essential that they focus on cryptosystems that make sense in classical number systems, such as the integers or real numbers. By restricting to classical number systems, less confident mathematics teachers would be working within comfortable bounds of knowledge and so, we hope, would feel more comfortable using these resources. These resources should also provide clear links between curricula and exam specifications which would allow teachers to see how this material will help prepare their students for exams and beyond.

A drawback to restricting to cryptosystems defined over classical number systems is that for many cryptosystems, the underlying security will be lost. However, the goal here is not to train teenagers to be experts in computer security, but rather to spark their interest in mathematics through real-life applications. Students will still understand the concept of cryptosystems: all that has been modified is the black box process. Specifically, for each cryptosystem studied, students will learn to encrypt and decrypt within the system enhancing both their understanding of the underlying mathematical concept, and the cryptosystem itself.

5 A sample topic for the classroom

Shamir’s secret sharing scheme (SSS) is a perfect example of a cryptosystem that preserves the underlying cryptographic structure over a classical number system and can be adapted to motivate and assess key learning objectives on a standard topic in secondary education: linear equations. In this instance, the learning outcomes would include recognising that a straight line is uniquely determined by two points, finding its gradient (or

slope), and finding the y-intercept.

For motivation, SSS can be adapted to a contemporary espionage problem like the following:

“MI5 wish to secure the combination to a safe so that no spy can access it alone, but any two can access it together. How can this be achieved?”

SSS stores a combination as the y-intercept c of a linear equation $y = mx + c$. ‘Keys’ are distributed to spies in the form of points on the line, one unique point for each spy. Since a linear equation is completely determined by two distinct points, see Figure 3, any two spies can use their keys to find the linear equation and reveal the y-intercept. However, an individual key, or point, alone does not reveal the linear equation.

For example, suppose two spies are given the points (8,262) and (17,361). Plotting these two points on a graph and drawing the unique line passing through them, see Figure 3, we see that the y-intercept is approximately 170.

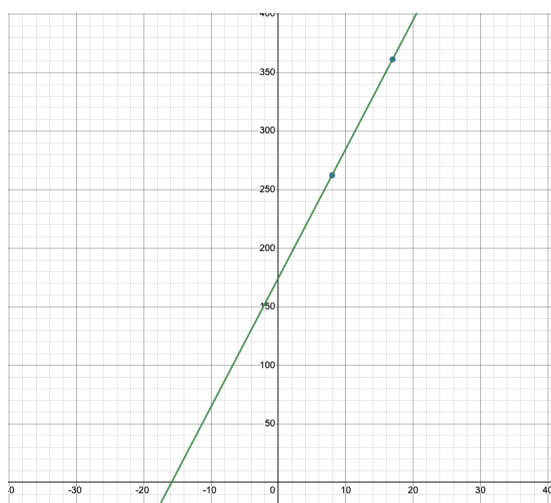


Figure 3: Line passing through two points

To find the exact combination, we need to find the linear equation. The equation of a straight line can always be given in the form $y = mx + c$, where m is the gradient and c is the y intercept. The gradient, or slope, is found by calculating the change in y with respect to x :

$$m = \frac{\text{change in } y}{\text{change in } x} = \frac{361 - 262}{17 - 8} = \frac{99}{9} = 11,$$

and so the linear equation is of the form $y = 11x + c$. To find the y-intercept c , we can use the fact that either of the points (8,262) and (17,361) lie on the line and so satisfy the equation. For example,

using (8,262) we get,

$$\begin{aligned} y &= 11x + c \\ 262 &= 11 \cdot 8 + c \\ 262 - 11 \cdot 8 &= c \\ 174 &= c \end{aligned}$$

giving a combination of 174.

This example is a highly specific illustration of how SSS can be used to highlight features of a linear function. However, it also offers a springboard for further discussion. For example, what other pairs of parameters could be used rather than two points? How can SSS be extended to higher degree polynomials? SSS is a perfect vehicle for exploring these questions as it can be implemented with higher degree polynomials to create higher threshold systems. For example, a three threshold system, where three points are needed to recover the secret, can be created using a quadratic function. Such exploration can be aided with the use of the open-source software, JavaCrypTool, (CrypTool, 2023) where SSS can be implemented and visualised on polynomials of any degree.

6 Conclusion

In our opinion, bringing cryptography to the secondary education classroom could significantly enhance student enthusiasm for mathematics, which may lead to increased student engagement. It is not, of course, without barriers. However, we believe these are eminently overcomeable with sufficient development of thoughtful and well researched resources appropriately adapted to ensure the mathematical content is of a suitable level for secondary school students and teachers.

We believe that if such resources were made available to educators, it would draw together the rich history of cryptography with the modern application of problem-solving and mathematical skills. Thus, learners would not only develop the ability to tackle real-world problems of the 21st century, but do so with historical perspective.

References

- Stephen J. Ball. 2003. The teacher’s soul and the terrors of performativity, *Journal of Education Policy*, 18:2, 215–228. <https://doi.org/fcvnnv>
- Stuart Boersma, Chris Christensen and Christian Millichap. 2024. Introduction to the Special Issue: Resources for Undergraduate Cryptology, *PRIMUS*, 34:1, 1-5. <https://doi.org/k9b9>

- Nigel Calder. 2013. Mathematics in student-centred inquiry learning: Student engagement, *Teachers and Curriculum*, 13. <https://doi.org/k64w>
- Pino Caballero-Gil and Carlos Bruno-Castañeda. 2006. A cryptological way of teaching mathematics, *Teaching Mathematics and its Applications*, 26. <https://doi:10.1093/teamat/hr1008>
- CrypTool Portal. 2023. Cryptography for Everybody. <https://rb.gy/1unnk1>
- Dell Technologies. 2018. *Realizing 2030 a Divided Vision of the Future*. <https://rb.gy/r19awk>
- Department for Education. 2023. *School Workforce in England*. <https://rb.gy/gqgy15>
- Robert E. Lewand. 2004. *Cryptological Mathematics*. Classroom resource materials, Mathematical Association of America. <https://rb.gy/oahy28>
- Ahmet Özdemir, Enes Güler and Nuh Aydın. 2011. Effects of Cryptographic Activities on Understanding Modular Arithmetic, *Turkish Journal of Computer and Mathematics Education*, 2(3), 247–256. <https://rb.gy/73ra38>
- Andrew Stott and Carmen Neustaedter. 2013. Analysis of gamification in education, [Unpublished manuscript] School of Interactive Arts and Technology, Simon Fraser University. <https://rb.gy/r7kbx1>