UNIVERSITY OF NEW SOUTH WALES

Unconventional Cryptography

Cryptology for Computing Students

Cameron Lonsdale
Bachelor of Science (Computer Science)

Supervised By
Professor Richard Buckland
Dr Roland Wen

A report submitted in partial fulfillment for
Special Project B - COMP3902

in the
School of Computer Science and Engineering

Monday 11th June, 2018

Declaration of Authorship

I, Cameron Lonsdale, declare that this report titled, 'Unconventional Cryptography' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research project at this University.
- Where any part of this report has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the report is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

“Our responsibility is to do what we can, learn what we can, improve the solutions, and pass them on.”

Richard P. Feynman

UNIVERSITY OF NEW SOUTH WALES

Abstract

School of Computer Science and Engineering

by Cameron Lonsdale

Computing university students are reporting difficulty learning cryptology primarily due to insufficient prerequisite knowledge and inability to apply concepts using their programming skill set. With more cryptography courses targeting computing over mathematics students it's important this content is tailored to maximise computing students learning. This report analyses the current situation of cryptology education in university coursework and external resources. It presents a set of criteria to guide cryptology educational development and - using this criteria in an empirical study (A MOOC course titled *Unconventional Cryptography*) - evaluates the approach. Analysis of students experiences show that tailoring cryptology towards computing students results in a higher level of engagement and understanding than traditional methods. Weaknesses were identified in the study regarding student motivation, strategies are suggested to better motivate the majority of students who were apprehensive in beginning their learning.

Contents

Chapter 1

Issues with Tertiary Cryptography Education

1.1 Student Experience

Over my time as a computing student at UNSW I encountered numerous students who complained cryptography was challenging to learn. For this project I wanted to understand why these students struggled, and whether this was a common experience.

I conducted a survey[1] of 35 students, the majority studying computing at UNSW (due to the surveys distribution[2]), and recorded that 68% of students had attempted to learn cryptography.

When questioned about their learning experience, over 70% rated their difficulty in understanding the content a 4 out of 5 or higher[3]. Why did the majority of students struggle? As one student summarises: "*The main issue i always had with crypto was the maths component*". For 44% of these students they specifically identified a lack of mathematics/prerequisite knowledge as the primary reason for their struggle.

[1] Raw results in Appendix A

[2] The survey was primarily distributed to UNSW computing students through UNSW only communication platforms (computing students making up the majority of recipients). However since the survey was easily accessible on the *Unconventional Cryptography* MOOC page (available to any logged-in student of the course) the collected data contained several responses from students not associated with UNSW.

[3] The uncontrolled variable in this data is that every student rated their difficulty based on experiences learning (potentially) different concepts in cryptology. One could argue not all concepts in cryptography are equally challenging to comprehend, therefore this needs to be taken into account when comparing students responses.

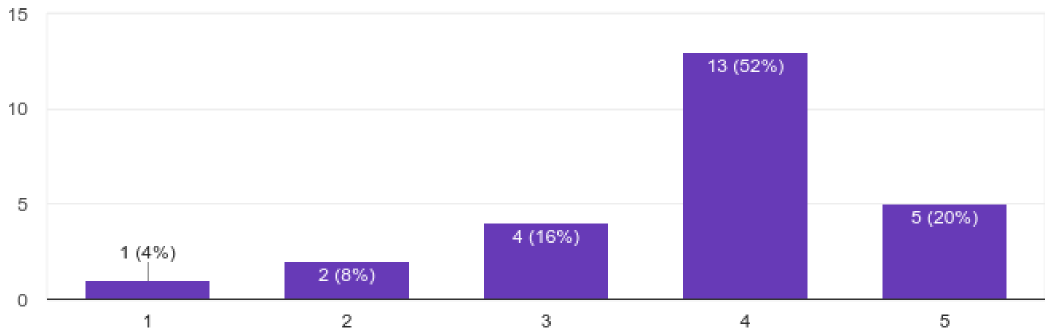


FIGURE 1.1: Distribution of difficulty experienced

Out of the students who experienced this level of difficulty, approximately 77% identified as having a university computing background[4].

Listening to the students it's clear that the majority struggled to learn cryptography due to either their lack of mathematical maturity, or mathematical concepts being ineffective in teaching. It is more likely however due to students mathematical maturity rather than the mathematics itself as students in the survey who claimed more experience with mathematics found cryptography easy to learn because of their background knowledge.

That being said, maturity with mathematics was not the only factor which determined a students success understanding cryptography; Several students who experienced a 1 or 2 out of 5 difficulty in understanding cryptography attributed their ease of understanding to *"Good resources and teachers + an interests in maths"*, *"a decent background in math and I spent some effort."* and *"I had good explanations and sufficient knowledge"*. Each student had a background/interest in mathematics, however factors of motivation, resources and teachers also influenced their experience. For struggling students they identified a whole range of reasons for their experienced difficulty, including laziness (*"was too lazy to understand"*), time management (*"Not enough time committed"*), understanding how to apply their knowledge (*"I experienced difficulties in trying to apply what I was being taught."*) and some even unable to understand why they struggled (*"i just cannot get my head around it"*).

All of these need to be addressed to better teach cryptography to computing students. This report will investigate the sources of these problem, describe how *Unconventional Cryptography* attempted to solve them, and then evaluate its success.

[4] Unfortunately due to an oversight when designing the survey I am unable to accurately identify particular students as computing students, this was due to the free response text field allowing respondents to identify themselves without structure. This is a lesson learnt. However because of the surveys reach and the types of students that would have studied cryptography I am confident in estimating that the respondents who did not identify themselves as maths students are most likely students of computing unless specified otherwise.

1.2 Cryptology Courses

First narrowing in on the students struggle with mathematics and the application of knowledge, to understand why these were an issue I surveyed[5] several American and Australian university cryptography courses to assess what faculty they belong to and whether their assessments are theoretical or practical in nature.

Out of 14 subjects analysed[6] 85% belong to the school of computer science[7] rather than the school of mathematics, and 57% include programming exercises as part of their assessment. It was surprising that the majority of subjects exist within the school of computer science despite cryptography traditionally being a mathematical discipline. One reason for this could be the association of cryptography with cyber security, which exists as a discipline within computer science, not mathematics.

1.2.1 Underutilised Teaching Methods

For cryptography subjects within the school of computer science only two thirds have a practical component (programming exercises), several still exist exclusively as a theoretical subject (mathematical theory questions). Despite students taking these courses having a programming background these skills are not always utilised as a teaching tool. From the ten students in the survey who had not yet attempted to learn cryptography, six of them answered similarly when questioned about their preferred method of understanding the content: *"Practical questions and Hands on problem solving"*.

Every computing course I have taken in UNSW has had some practical component where I applied my knowledge through code. This activity tested my understanding and allowed me to identify gaps in my knowledge. According to unofficial subject rankings[8] by UNSW computing students, one of the most hands on courses is also one of the most popular: Advanced Operating Systems.

Looking at other domains of knowledge, when you learn how to paint, you don't just theorise how to paint a picture, you pick up a brush and you try. In music, in addition to learning about music theory you put it into practice by composing and performing. In medicine, you practice your knowledge, in electrical engineering you build circuits. Across many knowledge domains practice is utilised as a teaching tool, but for cryptography, what's practised is the mathematics, the implementation side is often neglected.

[5] Raw results in Appendix B

[6] The number of subjects assessed was restricted to courses which had their coursework available online. Courses without lectures and assignments publicly available were discounted.

[7] Not all schools identified as Computer Science, more commonly they were Computer Science and Engineering. This has been simplified for ease of analysis.

[8] Dan's Comp Electives

There is a problem here, students are failing to see the application of their cryptography knowledge because it is not always being applied. Computing students (the majority of students that would take courses in the faculty of computing) are not always given the opportunity to learn through methods which they are comfortable and adept in: solving problems through code.

1.2.2 Inadequate Assumed Knowledge

Even though computing has its roots in mathematics, and students are often required to complete mathematics courses as part of their undergraduate degree, the survey indicates many computing students are not mathematically mature. For those that experienced a high difficulty learning cryptology almost half attributed this to their struggle in understanding mathematics.

For students who indicated they had not tried to learn cryptology, 44% reported the main barrier preventing their learning was the mathematics background required to engage with current cryptology educational resources. *"I am not very good at Maths"* one student commented; Another responded *"[There was] No good intro without a ton of prior knowledge required - mostly the maths"*.

To understand this issue from a low level perspective I conducted an interview with an educator from the Cryptography and Information Security - COMP343[9]course at Macquarie University to learn about students experiences. I learnt that the course ended up *"cut[ting] down a lot of the mathematics"* because *"students have problems with math"*. The reason for this? *"most comp sci students shy away from maths"*, *"they have done 2 semesters of discrete math previously but some students just pass that course without understanding things"*. And students struggle to understand the cryptography because *"the crypto part is still taught very traditionally, like a mathematics course"*. Additionally, all the examinations and exercises are theory based; Algebraic manipulations. And very little cryptanalysis is taught.

Upon examination, it is likely computing students struggle with the mathematics because they are not meeting the prerequisite knowledge current courses assume. For some students without mathematics as part of their degree, this is understandable, however for students who have to take mathematics courses in their degree, it's unclear why these have not given them the sufficient experience to understand mathematical cryptography. Perhaps the courses are ineffective in their teaching, or simply that this knowledge was not used by students in the interim and was forgotten. Whatever the reason, students are

[9] Transcript in Appendix C

unprepared to digest mathematics and cryptography courses are incorrectly assuming they are.

The question now is: Do you spend time teaching these students the prerequisite mathematics? Or do you try to teach cryptography using non-mathematical concepts? Perhaps a combination of both is most effective. This is a question we must research to determine how to best teach these struggling students. Although not a direct outcome of this report, it will attempt to answer this question given the existing research and newly gathered data from my experiment.

Chapter 2

Techniques for teaching Cryptology to Computing Students

Although computing students reportedly struggle to learn cryptology they have a strong desire to understand the content, whether be *"for fun"*, *"to solve crypto challenges in ctfs"* or *"for work"*[1].

Because the majority of students experience difficulty with the subject, modern cryptology education needs to embrace techniques for effectively teaching these students, specifically targeting the content and delivery. I argue an effective cryptology educational resource for computing students should be developed using the following principles:

1. Teach cryptanalysis alongside cryptography with the same prominence (P1)
2. Use practical programming questions to enhance student learning (P2)
3. Explain concepts using methods accessible to students (P3)
4. Have emotionally engaging material and encourage a community (P4)

[1] Taken from answers to the "If you want to learn Cryptography, what is your motivation?" survey question

Chapter 3

Related Work

Cryptography as a subject has been taught either as an integrated or standalone course for at least the last 20 years[1]. Despite this history there exists very little academic research on the effectiveness of different teaching methods for cryptography. Using what's available we can try to piece together an insight into the successfulness of different techniques used to teach cryptology and security in general.

3.1 P1. Teach cryptanalysis alongside cryptography with the same prominence

Without cryptanalysis, cryptography from the lens of security is all about thinking with a defence mindset. Learning to discover and exploit weaknesses in cryptography - cryptanalysis, I argue enhances a novice students understanding of cryptography above others without this knowledge. Not all topics in cryptography will apply to this rule, specifically this should apply to the main topics a novice student will learn in an introductory cryptography class, including basic symmetric cryptography, asymmetric cryptography and cryptographic hashing.

Temkin[1] (2007) reflected on his experiences teaching cryptography to computer science masters students. It was his belief that "*once students learn the ideas behind algorithms used in breaking codes they will be much better prepared to understand how to securely implement these algorithms*" (p. 3). Feedback from the students indicated they recognised learning cryptanalysis enhanced their understanding of cryptology (p. 7).

The P1 hypothesis is narrow and therefore research is hard to come by, however we can utilise research from the general security education community to help substantiate our

[1] NYU has run Design and Analysis of Cryptographic Protocols since 1996

claim. We can expand our original hypothesis to the claim that learning how to attack systems allows you to better understand how to protect them. Schneier[2] (2008) refers to this as the security mindset, the absence of which will result in insecure systems.

Over the past 8 years several empirical studies have been conducted to assess the educational benefit of teaching an offensive mindset. Mink and Greifeneder[3] (2010) conducted an experiment which educated one group of students defensively and the other offensively, then measured student performance with theory examinations. Their results showed students educated offensively scored higher overall than those educated defensively.

Yurcik & Doss[4] (2001, p. 6) found similar results when investigating experiments at Chalmers University, they concluded that *"While the goal is to learn about protecting systems against skilled attackers, this is best accomplished with insight into the methods and mindset of attackers - you need to know how to attack to defend well"*.

Important to note is the balance of both attack and defence education, they accentuate each other, but one cannot completely replace another. This was highlighted by Hooshangi, Weiss and Cappos[5] (2015, p. 5) who assessed students ability to practically attack and defend software programs. For an individual who had a strong defensive ability, there was a correlation with their ability to attack. This is expected as to defend well you need to first understand how you are weak and then fix the weaknesses. To attack well you need to first understand how you are weak and then exploit the weaknesses, both mindsets share the first step. However they determined there was no reverse correlation between the ability to attack and the ability to defend. Although both methods share the first step of identifying weaknesses, fixing vulnerabilities takes arguably more effort than exploiting. It is engineering which builds good software and engineering which is required to fix software. This skill is not common to all security students and therefore it is understandable that without it you can be a good attacker, but not a strong defender.

Across most research there is a strong indication that teaching the offensive perspective does lead to a better understanding of defensive security, therefore there is a high possibility that teaching cryptanalysis will also lead to a better understanding of cryptography.

3.2 P2. Use practical programming questions to enhance student learning

Practical cryptography depends on software and hardware implementations. I argue teaching students how to implement cryptographic concepts and cryptanalytic attacks will not only better educate them about domain specific issues (like Side Channel Attacks) but also enhance their understanding of cryptology over students without this experience.

When Temkin[1] (2007, p. 2) taught cryptography to students with strong programming backgrounds he noted *"The problem of keeping a balance between the amount of maths in the course on cryptography and the students' ability to understand is a delicate issue"*. He found that often these students would use their programming skills to assist in understanding the cryptography. But does this lead to a better understanding? To answer this we need to expand our scope more generally to include research about learning security through practice.

Cheung, Cohen, Lo and Elia[6] (2011, p. 5) facilitated university students to learn security through what is called Challenge Based Learning (CBL), where they competed in CYSCA-like cyber security competitions and CTFs. Before learning, on average students self reported their security skills a 3.7/10, after the study this increased by 92% as students rated themselves a 7.1/10 on average. However there are other factors which could have influenced this result, in particular the researchers note that group dynamics played a key role in the students enjoyment and effectiveness of their learning. Additionally, challenge based learning did not produce a strong level of improvement in all students, they noted that students who had a high motivation and interest in the program performed better than those who did not - indicating that for unmotivated students, challenge based learning will most likely be ineffective.

Sa[7] (2014, p. 12) conducted an experiment at King Abdulaziz University where they incorporated practical offensive security coursework into their undergraduate Computer and Information Security course. Surveys showed 78.38% of students taught believed that practical exercises helped them better understand security principles. A similar proportion of students believed it would be challenging to understand security attacks without implementing them. While this research reports a strong correlation between practical exercises and learning security, the students were new to security, and therefore were unable to compare this experience to a purely defensive education; The students were also not selected at random, the cohort consisted entirely of female students. Additionally the work was conducted in small groups, not individually. Therefore it's important to recognise these results may have been influenced more by the group work rather than the practical exercises, and that students may have biased opinions given their (lack of) prior experience.

In Greece, Papanikolaou, Karakoidas, Vlachos, Venieris, Ilioudis and Zouganelis[8] (2011, p. 5) developed an open source offensive practical tool to aid exercises for web application testing. Student survey results showed 85% of them thought that it helped them significantly in being informed about and/or understanding better the security issues each exercise was addressing. There are similar limitations in this research as Sa's, firstly we do not understand the background knowledge of the students and secondly this work was conducted in groups. This experiment was also run across different universities and their results combined, without taking into account how the different conditions, teaching staff and learning culture in each institution might affect student performance and experience.

Trabelsi and Ibrahim[9] (2013, p. 8) presented a case study that taught DoS attacks through offensive practical exercise. The researchers measured that 85% of the students believed the lab exercises to be useful and helped them better understand the underlying theoretical concepts associated with the attacks. While the practical exercises are well documented, little is said about how students were given the exercises, for example if it was in groups or if it was for an assignment or self learning.

On the surface, several experiments teaching practical security report a strong correlation between student understanding and learning through practical exercises. However one big limitation of this research is that it is subjective based and provides little discussion around the biases that might influence students opinions. Also, most of the practical exercises were completed as group work which could significantly impact the effectiveness of the exercise. Further research in this field needs to conduct more objective experimentation, with a more in-depth analysis considering all possible variables and producing measurable results which test student learning.

3.3 P3. Explain concepts using methods accessible to students

As we have seen, not all students willing to learn cryptography are able ascertain meaning from mathematical equations and concepts. However cryptography is largely a mathematical discipline, is mathematical maturity required to grok cryptography? Or are concepts able to be communicated through illustration and analogy.

Koblitz[10] (1997, p. 326) explored teaching cryptography to over 1000 high school students through physical group games and puzzles. Even with teaching maths heavy cryptography concepts like RSA, students reported an increased interest in cryptography and a solid grasp on the concepts taught. The author describes the content taught as "Kid Crypto", defined as "the development of cryptographic ideas that are accessible and appealing (and moderately secure) to those who do not have university-level mathematical training". Again, this experiment was conducted on groups of students, not individuals and the research provides little evidence to substantiate their claim.

Similar results were reported by Hamey[11] (2003, p. 8) at Macquarie University where students were optionally exposed to learning secure communication through an interactive game platform. Hamey discovered that students who used this platform scored higher on examinations than students who did not, possibly indicating the effectiveness of the game representation in communicating cryptography. We are unable to know what questions they were assessed on to determine what bias may have influenced students ability to answer the questions in the exam. This experiment was also conducted in small groups where students worked together on the exercises.

Bultel, Dreier, Lafourcade and More[12] (2017, p. 2) suggest teaching students without a strong background in mathematics or computer science can be done through relatable analogy and illustration. They detail child friendly explanations and boast their 10+ years experience teaching security courses as evidence these techniques have been helpful in communicating cryptography. From a scientific perspective this is insufficient evidence to support their claim, they do however detail the lessons to allow for a replication study. More scientific experimentation is needed to assess the effectiveness of these techniques.

Bell, Thimbleby, Fellows, Witten, Koblitz and Powell[13] (1999, p. 14) attempted to explain cryptographic systems to children and non technical adults through simple activities that require active participation. The activities use only basic arithmetic, elementary puzzle-solving and do not require the use of a computer. The authors reported that *"many of those who participate reach an understanding of what [is] generally regarded as advanced cryptographic techniques"*. They also found that these activities were carried out with enthusiasm from both old and young participants. Similar to the previous paper little evidence is given to support their claim. Interesting to note that they reported success through interactive exercises, where students conversed and worked together.

Several educators have claimed teaching cryptography without mathematics is highly effective, but does the level of understanding reached compare to an understanding which comes through learning the mathematics?

Although Temkin[1] (2007, p. 7) was able to teach students using programming exercises he spent many weeks teaching the background mathematics to increase the students maturity. One student commented on this saying *"Having the understanding of* *the mathematical foundations for the protocols will be helpful to truly understand how the protocols should be used and how they might be compromised"*. Temkin taught his cryptography course over two semesters instead of one; While he could afford to spend time improving the mathematical maturity of his students, not all courses have that luxury.

Holden[14] (2004) had a unique experience as he taught two cryptography courses, one aimed at maths and computing students, the other at non-technical students. For the non mathematics students he *"made an effort in the course to engage the students by bringing in examples from their daily lives"* (p. 1), they studied the maths behind crypto systems but also *"the impact that the invention of modern cryptographic systems has had and will have on political, economic, philosophical, and sociological aspects of society"* (p. 2). To achieve this his classes each week were segmented into maths, technical and social sections. The goal with the maths segment was to teach enough mathematics to understand RSA cryptography, which was a struggle for most students. Like myself Holden has the opinion *"More mathematical sophistication would have made the course easier, but I feel that it was important to teach a course which students of all backgrounds could take"* (p. 3). Holden tried group work but quickly found difficulties with students plagiarising others.

In the course with the technical students Holden was able to cover much more in depth technical knowledge due to the students mathematical maturity, however he noted *"Most students found the mathematics part of the homework more difficult than the computer science part, which was not surprising since most were computer science majors"* (p. 11). Holden concluded saying how striking it was that the same content can produce two different courses depending on the emphasis of the instructor and the ability of the students. The more technical students had a better grasp on the technical aspect of cryptography, but the non technical students grasped the social aspects better. Holden had hoped to demonstrate the value of teaching technical material to interested students without the necessary background; It was clear to him that a stronger technical background does lead to a better understanding of the material. However he felt that teaching the technical aspects of crypto to non technical students enhanced their understanding of the non technical aspects (p. 13)

One thing which remains inconsistent amongst the research is the competency in cryptography that was measured. Without this everyone's definition of effectiveness is inconsistent, and therefore we struggle to compare teaching methods. It is unknown to what level of ability the teachers expect their students to reach with their methods of teaching, is it enough to have students be able to pass an exam? Or do we expect them to be able to demonstrate a mastery of the concepts. From what Holden observed it's possible that different ways of presenting the content enhance students understanding differently, possibly in a way that it cannot be directly compared. For instance, teaching cryptography through mathematics provides the students with a level of understanding which is unable to be delivered through alternative illustrations of cryptography. Likewise the reverse could be true as well. Perhaps the best solution is to use both techniques. Without further research we cannot be sure, but existing research hints at this conclusion.

Another issue with all of these papers is that their experiments cannot be reproduced (easily), and their results cannot be verified. Therefore we cannot conclude that the alternative teaching methods are more effective, with further rigorous scientific experimentation, it could be possible to draw more concrete conclusions.

3.4 P4. Have emotionally engaging material and encourage a community

No matter how much effort you put into the effectiveness of your material, if students are not interested or engaged to learn then the material doesn't help any student. From surveying students it wasn't just the technical content which prevented them from understanding cryptography, but also human and emotional aspects relating to motivation and time management.

Many of the successful experiments looked at in the above sections share a common theme in how students work. Students work in groups to complete the challenging exercises put in front of them, and when they do it's observed that they help each other, come up with innovative ideas and overall feel more engaged. Bonwell and Eison, 1991 (as cited in Conklin[15], 2006) reported that *"an interactive component that forces interaction with others as part of the learning experience increases the effectiveness of the class in developing student skills"*. More specifically for online courses: Anderson (2006), Arbaugh (2000) and Garrison, Cleveland-Innes (2005) as cited by York and Richardson[16] (2012) conclude that *"Interaction is a critical factor that impacts student learning and motivation to learn in online courses"*.

In the year 2000, Garrison, Anderson and Archer[17] published what is known as the Community of Inquiry (CoI) framework, a set of 3 principles which are essential to the online educational experience: social presence, teaching presence and cognitive presence. Social presence refers to the degree to which learners feel socially and emotionally connected with others in an online environment; teaching presence is defined as the design, facilitation, and direction of cognitive and social processes for the realisation of personally meaningful and educationally worthwhile learning outcomes; and cognitive presence describes the extent to which learners are able to construct and confirm meaning through sustained reflection and discourse (York & Richardson[16], 2012). According to these definitions, my principles P1, P2 and P3 cover teaching presence as they refer to the design of how students learn information. However social and cognitive presence are facilitated by this last principle. *"Social presence marks a qualitative difference between a collaborative community of inquiry and a simple process of downloading information, When social presence is combined with appropriate teaching presence, the result can be a high level of cognitive presence leading to fruitful critical inquiry"* (Garrison et al[17] , p. 96). Not only does social presence lead to enhanced inquiry but the emotion associated with social presence is *"inseparably linked to task motivation and persistence, and, therefore, to critical inquiry"* (p. 99). Researchers Tu and Mcisaac[18] (2002) even argue that social presence is the most important factor in improving instructional effectiveness.

An essential component of the effectiveness of social presence is group cohesion. Cohesion and belonging are paramount for the collaborative experience (Garrison et al[17], p. 101), however there is the possibility for groups to decay and relationships to sour which could negatively impact students learning experience. When community works it works well, when there is dysfunction it tends to have the opposite intended effect. More research needs to be done on cultivating positive communities and how educators might go about maintaining the cohesion of their online class.

That being said I think there is an indication that social presence in an online course can enhance student learning, especially when working in tandem with effective teacher presence.

Chapter 4

Prior Work

With an understanding of the issues in cryptology education, I decided to survey several resources subjectively under the lens of a novice student and combine this with community feedback to determine which aspects of a resource resonated most with students. This analysis will be influential in the design of my online course: *Unconventional Cryptography.*

4.1 Practical Cryptography

Practical Cryptography[19] is an online lesson based website which teaches classical cryptography with a focus on practical application. The writing style of the resource is conversational and informal, making it engaging to read. The practical component manifests as JavaScript examples you can interact with, as well as semi-guided implementation steps to coding cipher breaking programs. The main drawback of this site is that the content is limited to just classical cryptography, additionally there is little challenge or feedback given to students. If a student wanted to test their knowledge, they would have to come up with the questions.

Judging from student feedback there is a positive response to the overall clarity and presentation of the content (Appendix D1). The majority of students find the resource informative and helpful, without needing further clarification (Appendix D4)[1]. The resource does use mathematical symbols to communicate concepts, which is not always well received (Appendix D2). *”It uses a level of math I'm not familiar with. I don't understand these variables”*. Interestingly, the author notes in one of their comments

[1] It's import to recognise with this and other feedback that there could be bias which affects whether a student leaves a review. Depending on the review and on the student, the reviews may be skewed in a certain direction because not all students are leaving their feedback.

that to intuitively understand the Atbash cipher, an understanding of the mathematics is required. This implies that he believes whilst core concepts can be communicated without maths, a lack of mathematical maturity restricts one's ability to appreciate cryptography (Appendix D3).

Using my criteria *Practical Cryptography* achieves most of P1, P2, P3 and P4. Cryptanalysis is given equal weighting to cryptography as evident by the content on the site; Practical exercises are given but so are the full solutions, you can debate the effectiveness of this decision but the resource does show students how to practically build and break ciphers. Additionally, the resource tries to be diverse in the way it explains content through examples, interactive elements and also mathematics. And lastly it engages students in a way they feel they can ask questions and contribute, as evidenced by the existing comments.

I used this resource to learn cryptology when I was starting out and found its instruction helpful. To design *Unconventional Cryptography* I used the writing style of *Practical Cryptography* as inspiration, and also used the content as a reference to compare against my explanations of classical cryptanalysis.

4.2 Cryptopals

Cryptopals[20] is a collection of cryptanalysis practical exercises. The challenges are aimed at novices and increase in difficulty as the sets progress. *Cryptopals* is minimal in terms of the level of detail it provides to solve the challenges. For some students this leads to confusion due to ambiguity, resulting in frustration (Appendix E1). *"I feel like an idiot getting tripped up on number 3 in the first set. They don't seem to give enough information"*.

Ultimately a lot of students find themselves with a decline in motivation (Appendix E3), *"I've been meaning to do the challenges at http://cryptopals.com/ for some time now, but can't seem to motivate myself"*.

For self-regulated learning, students self efficacy and task value beliefs can determine their level of motivation[21] (Pintrich 1999, p. 9), for some this can lead to a drop in motivation and suspension of learning. For students who remain motivated they recognise the learning potential of the challenges (Appendix E2) which substantiates findings from research on challenge based learning. *"First of all, I swear by Cryptopals. They are what made me realize I get, like and can do cryptography. They are just the best programming/math/crypto/anything challenges I've ever played, and one of my first and most satisfying accomplishments"*.

Interestingly, in response to the difficulty, students formed study groups to aid each other in their learning (Appendix E4).

Using my criteria, *Cryptopals* achieves only P2. The resource is too one sided towards cryptanalysis, the cryptography content you must source externally (P1). For this reason some students get frustrated, which you can argue negatively impacts their engagement (P4). This frustration however did lead them to find a community to solve their problems, by forming study groups. For P3, what's presented to the students is accessible without much mathematics background (as was intended by the resource), although the content is minimal, with their intent being that students will go and learn most of the content elsewhere.

For *Unconventional Cryptography*, I aimed for it to have the same quality of practical activities which teach students how to break real world crypto. However the main difference will be the level of instruction given to students. Because my target audience is novices, my challenges will provide enough guidance to aid students in completing them, rather than the extreme of letting students find out everything by themselves. My hypothesis here is that this will help retain student motivation and prevent a decline in student progress.

I used *Cryptopals* throughout the development of this course to teach myself more advanced cryptographic attacks, such that I may then teach the students.

4.3 Serious Cryptography

Serious Cryptography[22] is a modern (2017) cryptology book written by Jean-Philippe Aumasson, creator of the BLAKE2 hash function. There is a distinct difference in the writing style compared to alternative cryptology textbooks. Aumasson writes with friendly language and a casual tone, it's less of an textbook and more like you're reading a story about cryptography. It talks less about the mathematics and more about the concepts. There is also example Python code to reinforce concepts to programmers.

The general feedback is overwhelmingly positive, specifically around the presentation of the content. *"Awesome. Well-written, approachable, and a really fun read"* . Common complaints involve readers feeling the content was rushed, or assuming prior knowledge which they did not have (Appendix F) *"It is difficult to understand without prior knowledge"*.

Serious Cryptography achieves P1, P3 and P4. It covers both cryptography and cryptanalysis with the same emphasis; The content presented to students uses written, visual and code explanations to communicate concepts; and lastly the book is written to be engaging. Being a physical, written medium limits its ability to provide practical challenges and also foster a community of students.

With *Unconventional Cryptography* I want to emulate the success of *Serious Cryptography* as much as possible, using it as a complementary resource to aid students in their learning and providing the interaction and feedback which the book is unable to deliver.

4.4 Stanford Cryptography I

Cryptography I[23] is an online course taught by Stanford Computer Science Professor and Applied Cryptographer Dan Boneh. The course has received over 331 5/5 positive reviews, the majority of feedback crediting the professor for his instruction in lectures. He is able to communicate difficult concepts effectively in short amounts of time. However these concepts require significant mathematical background knowledge[2]. It is a course heavy on theory and for these reasons it struggles to teach novice students who are looking for an easier introduction with practical examples. *"Should have come with an explanation that non IT background people cannot apply"*[3], *"Really tough math wise for me, having come into this straight out of high school"*[4], *"I did look at the coursera course on cryptography and put it on the backburner when I was two videos in and realised I had no idea what the maths symbols meant"*[5].

Using my criteria *Cryptography I* achieves P1 and P4. Boneh does an excellent job describing both cryptography and cryptanalysis, however there are few practical exercises for the student, it's mostly comprised of theory questions. It relies on an over emphasis on mathematics to teach cryptography which may be its intent but by doing so alienates students without this background knowledge. But students are engaged by the content, particularly the lecturer and his delivery; Students are comfortable asking for help and helping each other in the forums.

I used this resource primarily to learn more about the theory of cryptography. Going through the content I was able to cross reference this with my knowledge on practical attacks to differentiate which content was and was not necessary for students to learn how to break crypto systems.

[2] https://www.coursera.org/learn/crypto#ratings

[3] From the coursera feedback

[4] From the coursera feedback

[5] From Appendix A survey

4.5 Cryptopals Streaming

In October 2017 Filippo Valsorda (a cryptographer at Google) streamed video[24] of himself completing the cryptopals challenges, this idea was met with anticipation by the public[6]. The benefit of using video to explain the *Cryptopals* challenges is that you gain an understanding of the problem from someone else's perspective. However as an educational resource the content was too long and unstructured to be used effectively. Teaching cryptographic attacks by using short tailored videos has the potential to be very effective.

Using my criteria this project achieved most of P1, P2, P3 and P4. What is missing in *Cryptopals* in terms of cryptography is added by Fillippo in his commentary while completing the challenges. P2 is a given as it is utilising the *Cryptopals* challenges. P3 comes in as you are receiving the content with verbal and visual explanations as well, allowing more avenues to convey the content to students. And lastly because it is an interactive event, students can comment, ask questions and learn together as Fillippo is progressing through the challenges.

Because *Unconventional Cryptography* is an online resource it can take advantage of video to demonstrate how crypto attacks are successfully executed.

4.6 Handbook of Applied Cryptography

The Handbook of Applied Cryptography[25] (along with similar books from the same time period) is one of the classic graduate level reference books from the 1990s. While the content is everything you need to know, it is written clinically as a reference book, not a book designed with student learning experience in mind. However this doesn't stop many *"best resources for learning cryptography?"* queries to be answered with the *Handbook of Applied Cryptography* (Appendix G)

Using my criteria, the *Handbook of Applied Cryptography* only achieves P1. It does describe cryptanalytic attacks in detail alongside the explanations of the corresponding cryptographic system. However there are no practical exercises (a challenge given the medium), the content is presented in a single perspective with little visual or supplementary aids (P3). And lastly the text is written as a reference book, not with student engagement as a priority (P4).

This is part of the problem to why new students find cryptography difficult, not just because there are few resources aimed towards them, but that the wrong resources are

[6] https://twitter.com/FiloSottile/status/787777267313303553

continually recommended to them over and over. Students *"[Do] not know where to start"* [7], and their first experience with cryptography should not be the *Handbook of Applied Cryptography*.

[7] A student responding to "Are there any barriers that have prevented you from trying to learn Cryptography before?" in my survey

Chapter 5

Course Design

Unconventional Cryptography aims to be the resource that computing students turn to when they first starting learning cryptology. The design of the course was guided by my four principles. The course teaches cryptanalysis as well as cryptography; It uses practical programming challenges to teach students; It teaches cryptography using diagrams, analogy, and mathematical equations; And lastly it's written to be emotionally engaging and allow students to form a community. I wanted the resource to teach students not only theoretical knowledge, but give them the skills to 'do' cryptography; to 'do' cryptanalysis rather than just theorise and describe it. The course also teaches modern cryptography including RSA and AES, in addition to classical cryptography.

Unconventional Cryptography was realised as a MOOC course on OpenLearning available to any student with an OpenLearning account.

5.1 Content

At the end of this project *Unconventional Cryptography* had the following lessons:

1. Classical Cryptography
    (a) What is Encryption
    (b) Caesar Cipher
    (c) Substitution Cipher
    (d) Vigenere Cipher
    (e) One Time Pad
2. Stream Ciphers

   (a) Breaking Stream Ciphers

3. Block Ciphers
   (a) What and Why
   (b) ECB

4. Asymmetric Cryptography
   (a) What and Why
   (b) RSA

5. Post-quantum Cryptography
   (a) What and Why

5.1.1 Structure of a lesson

The structure of each lesson differed depending on the content, however the cipher oriented lessons all followed a similar structure:

1. Cryptography
   (a) Overview
   (b) Example
   (c) Optional Mathematics
   (d) Programming Exercise

2. Cryptanalysis
   (a) Overview
   (b) Example
   (c) Theory Question
   (d) Optional Mathematics
   (e) Programming Exercise

The lesson was divided into two segments, cryptography and cryptanalysis, both of equal prominence (P1). Both segments included a practical programming exercise for the student to learn how to implement the cipher and break it (P2). Where possible the concepts were explained without the need for mathematical symbols, but this was included optionally for students who desired that knowledge (P3). The content was written to be emotionally engaging, and the platform provided students with the ability to interact with the resource and each other to foster a community (P4), that being said the course was not designed to specifically encourage students to build a community or work together.

5.1.2 Deciding what to teach

Deciding what and what not to teach was primarily guided by principles P1, P2 and P3. But certain topics were left out of modules for two reasons. Firstly, due to time constraints certain lessons could not have been written before the conclusion of the project. Secondly, not all lessons in cryptography are considered essential for teaching the key principles and concepts that novices need when starting to learn cryptography. The lessons in *Unconventional Cryptography* were chosen by taking into account my own experience learning cryptography as well as research into prior work, for example a lesson on transposition ciphers was not included in the Classical Cryptography module because I felt the concepts taught were already covered throughout existing lessons in that module.

Decisions also needed to be made regarding the level of detail I described the practical exercises to the students. Learning from challenge based learning research, Cheung et al[6] (2011, p. 5) reported that for students who were not motivated to learn, challenge based learning was ineffective. For motivated students however the learning benefit was substantial. Therefore my resource has the potential to have a large drop off in participation from students who have little motivation. Additionally, Yurcik and Doss[4] (2001, p. 6) observed in practical challenges, common student complaints were about the lack of instruction and direction, however this was by design to encourage student self learning. From my personal experience outside of this project, for students without the motivation to be self learners, being asked to complete open ended style challenges often led them losing their motivation to continue using the resource as they preferred detailed instruction and direction. With this in mind I made the decision to provide detailed instructions and direction in practical exercises in an effort to maintain student motivation.

5.2 Delivery

The content of *Unconventional Cryptography* is delivered primarily through the written word, the main reason for this was that I was most comfortable using this medium and felt like I had the most potential for success in embodying principle P4. I did want to use videos and animations to teach the content but due to lack of time and shifting priorities I was unable to explore the effectiveness of those mediums. Each lesson is written conversationally, almost like a transcript from a lecture. There is evidence which suggests people prefer informal writing when reading text on the web because it's easier to parse: *"I prefer informal writing, because I like to read fast. I don't like reading every word, and with formal writing, you have to read every word, and it slows you down"* (Morkes and Nielsen[26], 1997). In addition, Ginns, Martin and Marsh[27] (2013) experimented with conversational writing styles and education to conclude that students who used instructional materials written in a conversational style learnt more than those who studied more formally expressed materials. Students also found this style to be more interesting and engaging to read.

The content of the course is delivered all up front, for students to complete at their own pace. This decision was made because there would not have been enough time in a single semester to both build and run a course of this scale. I do have concerns about displaying all the content at once, it's possible students could see that and be put off by the volume of work to complete the course. The amount of time needed to invest could result in students not starting at all.

5.3 Feedback

Unconventional Cryptography has tests in each lesson which help students assess their own understanding. Because the course is self paced each test needs to be auto-marked such that students can check their understanding without an instructor. Because of this requirement it limits what exercises you can use to provide feedback to the students. Short answer / multiple choice can be auto-marked and these are good for theory questions where you want to test a students ability to remember and comprehend what they just learnt. However, the goal of Unconventional Cryptography is to also teach students the ability to implement cryptography and cryptanalytic attacks, to test students against this in an automated fashion, it adopts a Capture The Flag (CTF) exercise format. Each exercise challenges the student to either implement or break a part of cryptography, once they have completed the challenge students will be able to recover a secret piece of text (also known as a flag) which they can use as a proof of their work. Submitting this secret string as an answer to the challenge proves students completed the challenge. This format allows us to verify students have demonstrated a skill without the need to manually check. That being said, similar to other styles of questions, CTF style challenges can be cheated on by students who will take flags off other students who have completed the work. This is an unavoidable reality which is only a detriment to the students learning.

Chapter 6

Key Decisions and Challenges

To better understand my hypothesis *Unconventional Cryptography* was developed with P2 at the core of its lessons. However this decision introduces the prerequisite of programming skills, which not every student wanting to learn cryptology will meet. As my focus was on teaching computing students, I made the decision to have programming as a prerequisite as I believe without it a student would receive a substandard understanding of cryptology compared to students who had coding skills. This course does limit itself to the number of students able to complete the course, however I argue it provides a higher quality level of understanding to the students who can take it, compared to existing courses.

As part of P3 I wanted to explain cryptography in such a way that computing students could understand, ideally without much mathematics. For certain lessons, like RSA, the mathematics is unavoidable. Research suggested explaining the content by using analogy could be successful, but because students would need to implement algorithms which utilised mathematics, they would need to be exposed to the equations regardless. Therefore I made the decision to explain content using mathematical equations but put effort into explaining all the symbols and concepts in English.

The decision to host the course on OpenLearning was made due to the need to collect student metrics in order to evaluate the successfulness of the project. The downside to this is that it adds an authentication barrier for students accessing the content, many students might not bother creating an account in order to take the course.

Chapter 7

Analysis and Evaluation

At the end of the 12 week semester a total of 176 students had enrolled in *Unconventional Cryptography*. The students came from geographically diverse backgrounds, with the total number of countries accessing the course reaching 26.

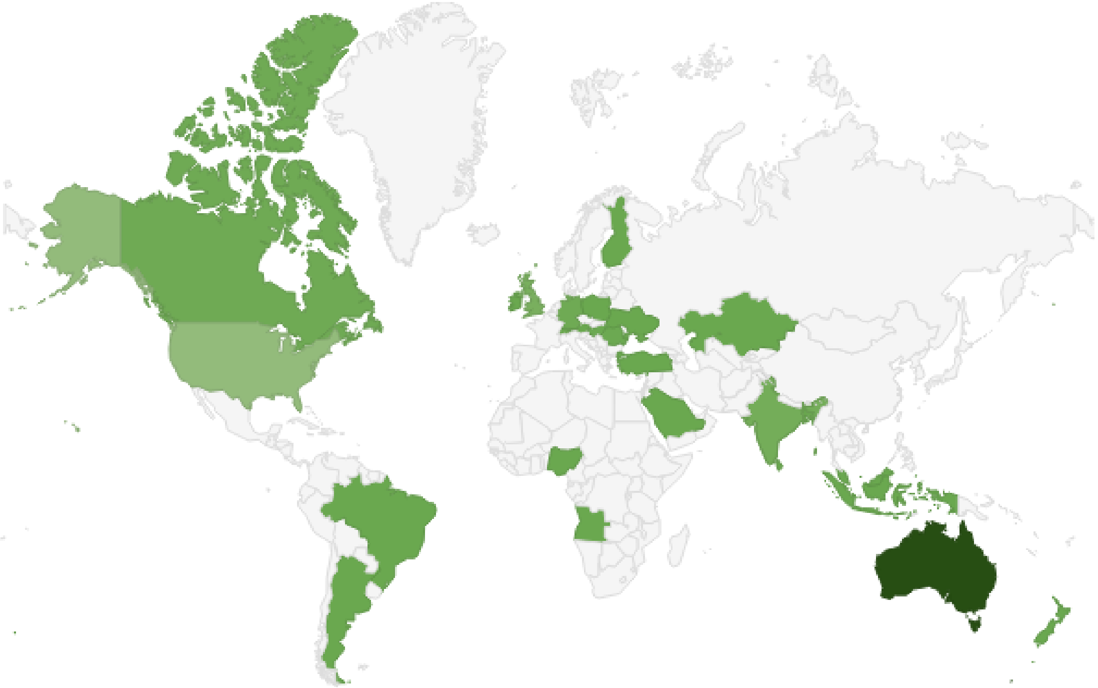


Figure 7.1: Geographic Distribution of Students
The darker the colour the more students

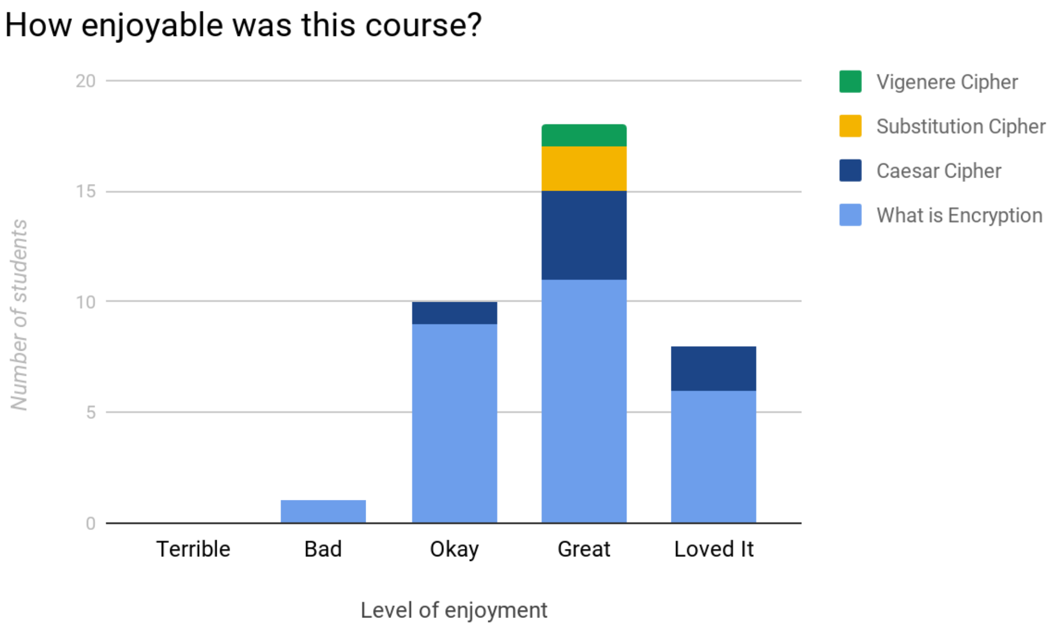
As students signed up to the course on their own accord, this is strong evidence to suggest that there is a demand for cryptography educational resources like *Unconventional Cryptography*. Despite the evidence that students struggle with cryptography, they still seek out ways to learn it.

7.1 Overall Student Experience

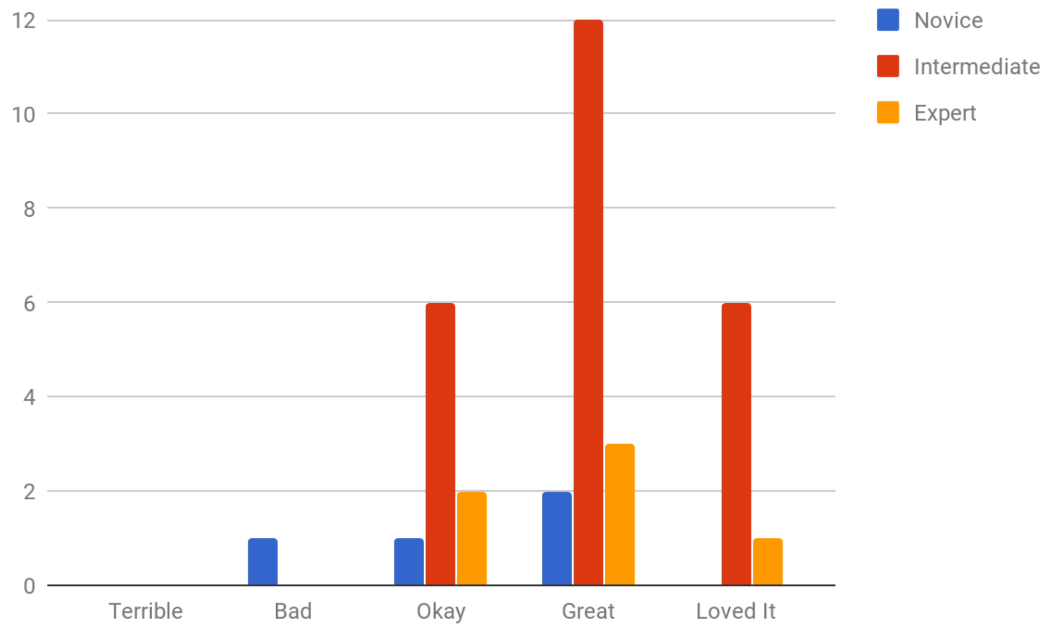
Each lesson in the course had a survey to allow students to submit their feedback about the lesson they just completed. Out of 12 lessons only 4 had completed feedback forms.

Lesson	Survey Respondents
What is Encryption	28
Caesar Cipher	7
Substitution Cipher	3
Vigenere Cipher	1
Total	*39*

As each survey is identical we can aggregate the responses to determine students overall impression of the course.

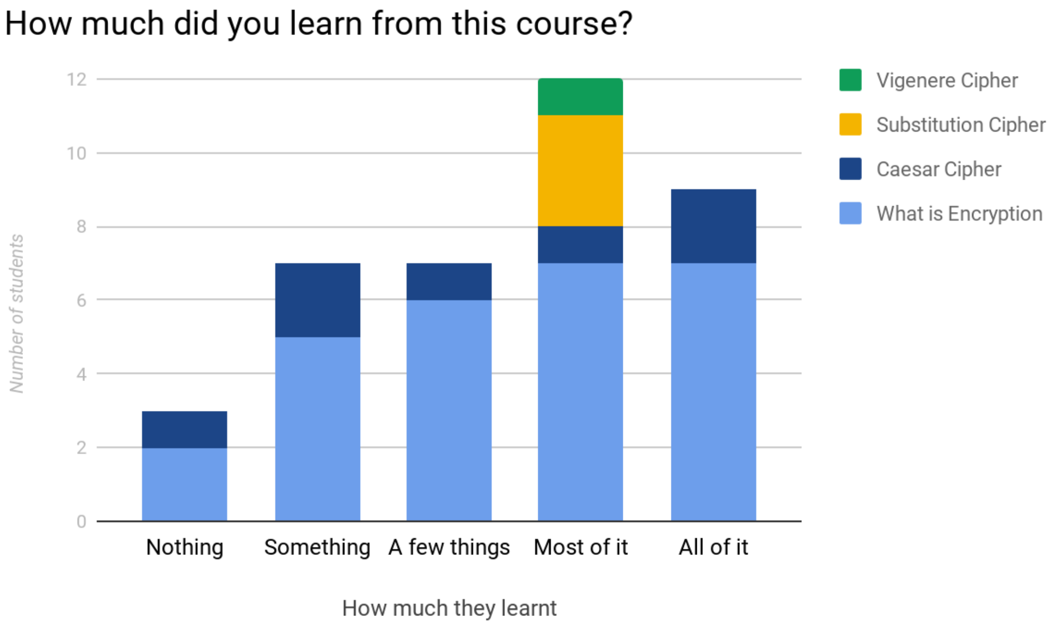


70% of students who answered the survey rated the course a 4 out of 5 or higher in terms of enjoyability, the phrases *"Great"* and *"Loved it"* indicating a level of positive emotional engagement with the course. Only one person had a negative emotional reaction to the course, this was a reaction to the lesson "What is Encryption" which was a minimal introductory lesson designed to explain the basics in simple language. As no explicit reasons were collected it's unclear why they reacted this way, It's unlikely due to frustration over them not learning anything new because they indicated they knew none of that content and learnt most of it from the lesson. Therefore the lesson was effective in teaching that student but perhaps not as engaging or entertaining as they might have hoped.



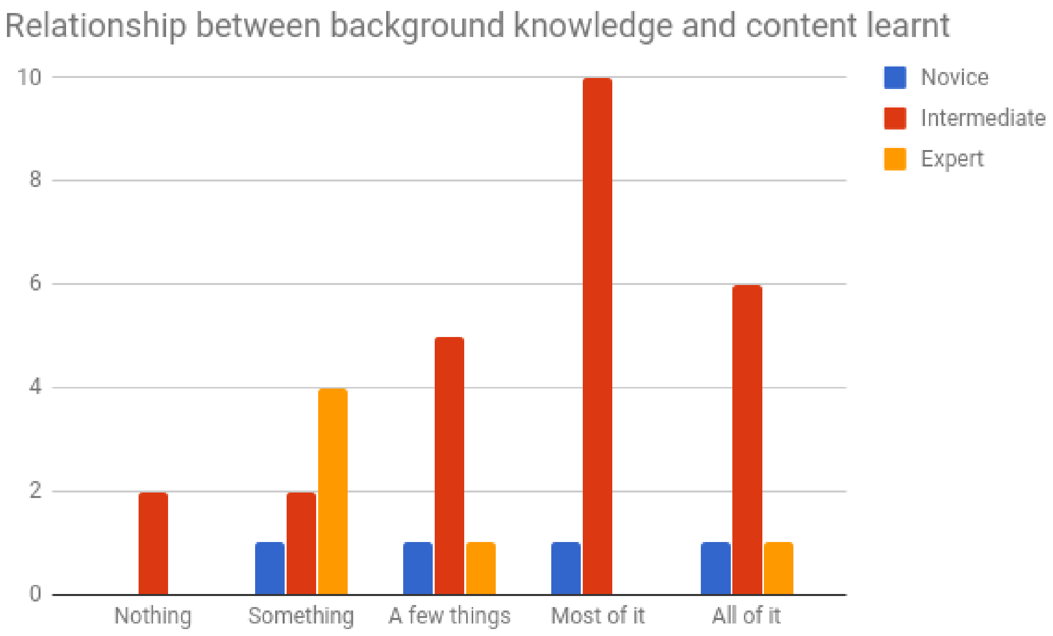
Most students rated their existing cryptology knowledge as ”Intermediate”, meaning ”I knew a couple things”, compared to ”I knew none of that (Novice)” or ”I knew all of that (Expert)”. The majority of intermediate students reported a 4 or higher in terms of enjoyability, this could be attributed to students having the combination of enough background knowledge to be able to easily digest the lesson, but also have room to expand their knowledge. Therefore they complete the lessons having gained the knowledge without having to exert large amounts of effort to meet the background prerequisites. This hypothesis could explain the behaviour of novice students as even though they had everything to learn they might not have met the prerequisite knowledge to be able to effectively absorb the content from the lessons. This is also substantiated from the survey data which reported two students stopped early on in the course as they felt they did not meet the prerequisite knowledge. For expert students, although they didn’t learn much from the lesson they still reported enjoying it to a similar degree as the intermediate students.

I would consider myself to be an intermediate student, and therefore when creating this course there is a slight bias to treat the students as though they are like myself; After all, I did create this course to be the course I wished existed when I was first learning cryptography. As a result, the lessons and how they were presented would most likely resonate stronger with like minded intermediate students, and although unintentional, may alienate novice students. This is a strong possibility for why intermediate students were the majority to complete the course, and why they enjoyed the course more than novices. The implication of this is that it’s quite easy for teacher bias to influence how content is taught and how effective it is at reaching different kinds of students. It is important for all teachers to recognise this and evaluate their own lessons to determine if you are assuming students are like yourself, or if your lessons are diverse in their teaching so as to reach all kinds of different students.



The effectiveness of the teaching resource is distributed slightly more evenly, of the lessons completed, the majority of students learnt most of the content within that lesson. 55% of students reported learning most or all of the content from this course, the others learning part of the content, and a small amount of students learning nothing. We can cross reference this data with the amount of background knowledge the students already had to see if the resource was effective at teaching cryptography.

The students who learnt the most content from the lessons were actually the intermediate students. Novice students varied between learning all the content, and very little. While most experts still managed to find something to learn from the lesson, despite having substantial existing knowledge in the field. A possible explanation why novices varied in absorbing the content is possibly due to their lack of background knowledge / skills. In most lessons I assume programming and basic maths skills which these students may not have all met, and therefore struggled to progress through the lesson. It is possible I thought my content was more tailored to novice students than it actually was and so, wasn't as effective in teaching them cryptology as it could have been. That being said, the survey response rate is low, and more novice student feedback is needed to confirm this hypothesis; Additionally students may have answered incorrectly for this data due to a misunderstanding of the question, it's possible students answered the



question considering how much of that content they already knew, rather than the delta between their knowledge prior to starting the lesson, and their knowledge afterwards.

7.2 Evaluation of the principles

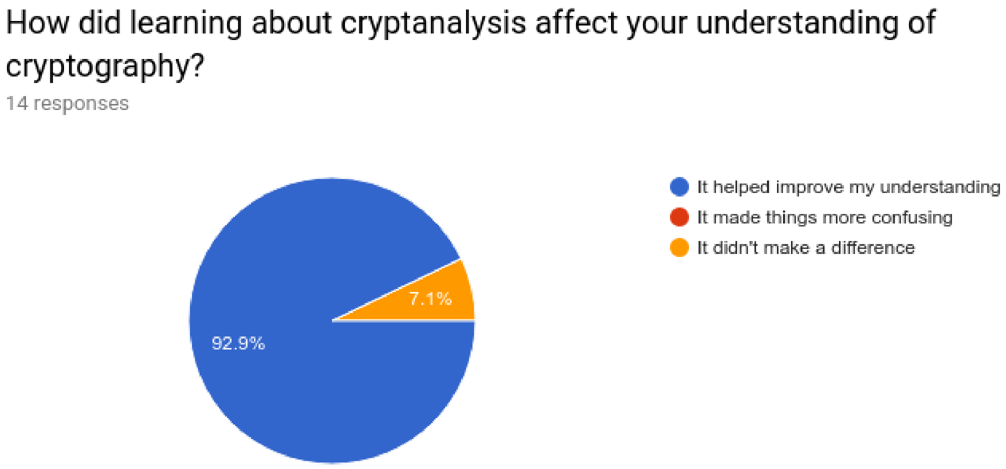
To evaluate the effectiveness of my four principles, all enrolled students were surveyed[1] about their experience.

7.2.1 P1. Teach cryptanalysis alongside cryptography with the same prominence

Out of 14 students who were asked how learning cryptanalysis affected their understanding of cryptography, 92.9% reported that it helped improve their understanding, 7.1% stating it made no difference.

The limitation here is that this data purely subjective and open to biases in students opinions. The majority of these students only completed exercises in the Classical Cryptography module and therefore have a limited perspective. More evidence is needed to confirm the objective educational benefit, but this evidence suggests a perceived benefit by the students.

[1] Raw results in Appendix H

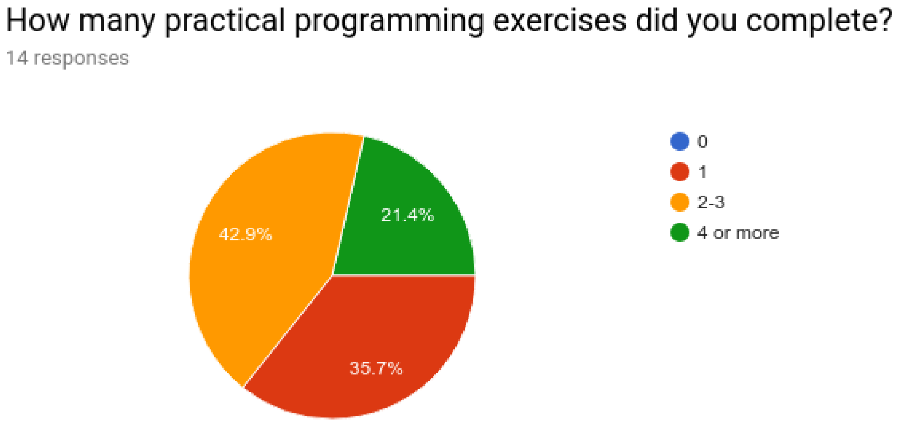


How did learning about cryptanalysis affect your understanding of cryptography?

14 responses

7.2.2 P2. Use practical programming questions to enhance student learning

The same 14 students ended up completing several practical programming exercises, the majority managing to finishing between 2 and 3 exercises.

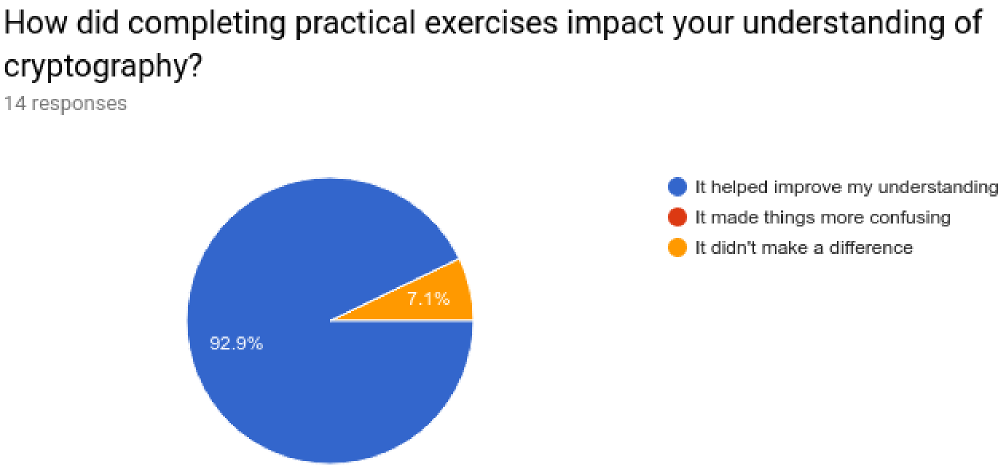


How many practical programming exercises did you complete?

14 responses

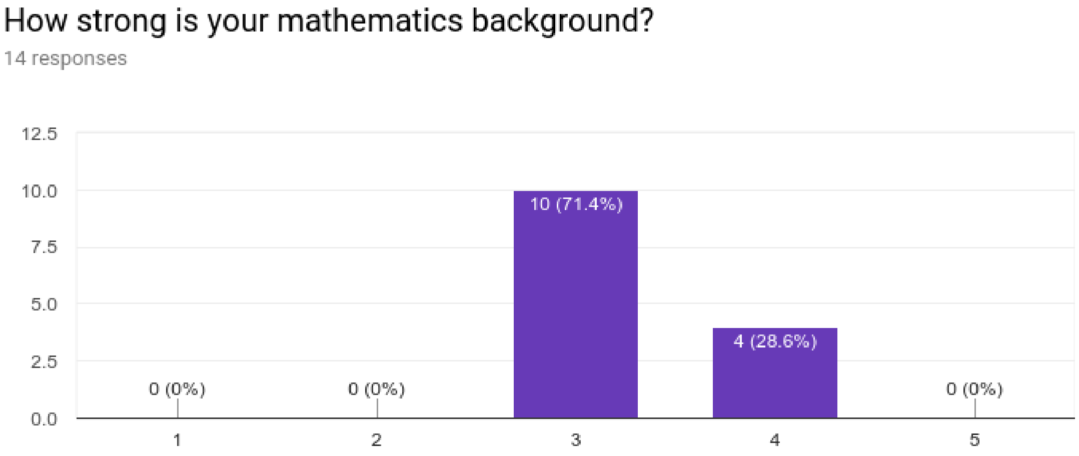
A similar 92.9% of students recognised that completing practical exercises helped improve their understanding of cryptography.

The limitations of this data are similar to those from P1, most students only completed practical exercises from the Classical Cryptography module, and this data is subjective, which is influenced by student bias. For future research this hypothesis should be confirmed with an objective study of skill, however this result does indicate a perceived benefit of using practical programming challenges to teach cryptography.



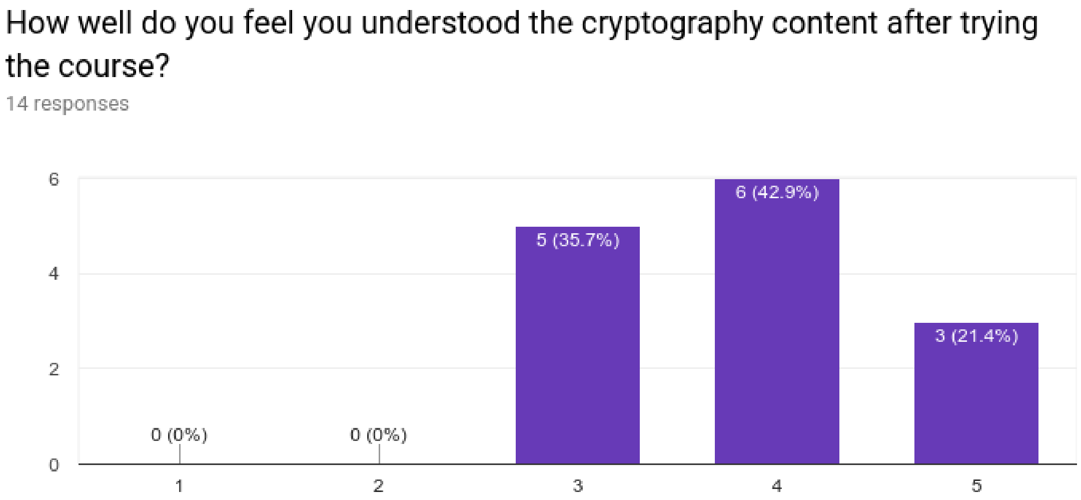
7.2.3 P3. Explain concepts using methods accessible to students

For the students who completed the course, they reported their mathematics background to be on average a 3 out of 5.



With this background, the majority of students reported they were able to understand the cryptography content quite well, rating their understanding a 4 out of 5.

Coupled with the data from the lesson surveys, the majority of students who took *Unconventional Cryptography* were able to understand the coursework without needing a strong background in mathematics. As most of the lessons completed were from the Classical Cryptography module, which is comparatively not a complicated mathematical topic in cryptography, this data is insufficient to answer whether a mathematics background is necessary to learn cryptography. If a mathematical background was the

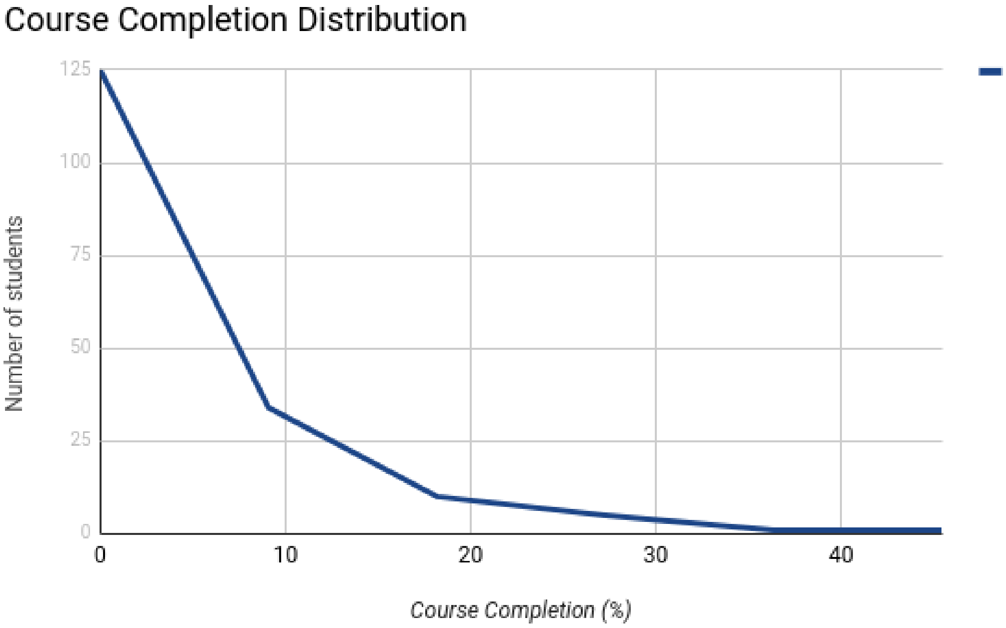


only indicator of success in learning cryptography than the majority of respondents would have answered 3/5 for their understanding (due to the average mathematical maturity of students being a 3/5); Given that most students report a higher score of 4 or 5 the content was able to be understood without the need for an equivalent mathematical maturity. Statistically, this is not a significant enough difference to provide a compelling argument.

The students who answered this survey were exposed to the mathematical topics of frequency analysis, index of coincidence and the chi-squared statistic, which was explained by using mathematical terminology (whilst also teaching the mathematics). The lesson which teaches most of this content, "Vigenere Cipher" has the lowest completion rate out of all the Classical Cryptography lessons, only 13.3% of students who viewed the lesson completed it, compared to 32% of students that completed the "Caesar Cipher" lesson after viewing. In the final feedback survey, the ineffectiveness in teaching those concepts were called out by one student who commented: *"I think frequency analysis should be better explained"*. I think this evidence suggests my efforts to explain cryptography by using/explaining mathematics was not as effective as I had hoped. I believe there is merit in teaching using mathematics to explain parts of cryptography but I was unable to explain the concepts using methods that were accessible to all students, because I failed to actualise P3 in *Unconventional Cryptography*. What could have improved this results was to take on board the feedback from the first student survey more closely and create *"Interactive elements and lots of short videos/animations"*, and other diverse ways of explaining the content in an effort to reach students who respond better to these mediums.

7.2.4 P4. Have emotionally engaging material and encourage a community

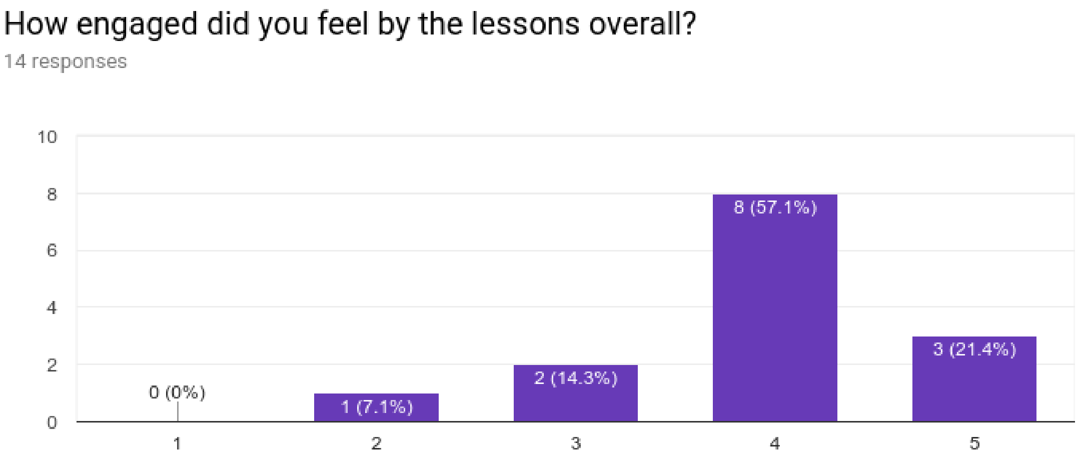
Despite a strong interest from students signing up to the course only 29% of students had started any of the lessons. Looking at the overall distribution of participation there is a steep decline in the number of students who progress throughout the course.



15 students who had completed 0% of the course were questioned about what prevented them from starting any of the lessons. For 93.3% the answer was *"I haven't had time"* which is understandable as the time frame in which the course was run coincided with a university semester, meaning most participants had their own university courses to complete. I feel as though this answer does not fully represent the opinions of the students, as, when questioned about what might encourage them to start the course only 26% of respondents mentioned having more time. For 47% of students, what would motivate them is the opportunity to work with others in a study group. 26.7% reported they would prefer videos to watch rather than text to read, and 13.3% said having shorter modules.

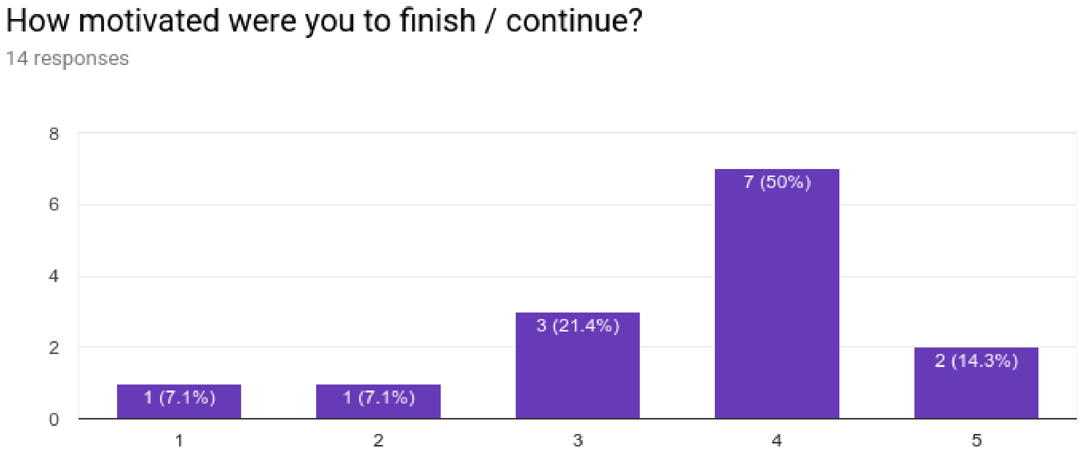
This contrasts with the opinions of students who had completed part of the course; When questioned what might encourage them to continue only 14.3% of students reported working in groups, the majority (64.3%) reported watching videos would motivate them to continue the course.

Although *Unconventional Cryptography* provided support for a sense of community through the OpenLearning platform, students were not encouraged or required to work together and create a community around the course. From the evidence it seems that this is one reason why many students were reluctant to start the course. As we have seen, the "intermediate" student is the one who was most drawn to start *Unconventional Cryptography*, by definition these students should have some prior experience and therefore some confidence in their ability to learn cryptography and progress through lessons as they have done so before. For novice students this is not true, which is probably the reason why 47% of students who hadn't started would have been more inclined to try the course if they could work together in groups. This result agrees with Garrison et al's[17] claim which states that the emotion associated with social presence is "*inseparably linked to task motivation and persistence*", meaning for students who lack the confidence in their ability to teach themselves, having a strong social presence could motivate these students to begin their learning as they have a supporting group of students to help them.



Students who have progressed through the course reported rather than working in groups, having more diverse and digestible mediums (videos) would assist them in progressing through the course. From our understanding it's reasonable that most of these students can motivate themselves quite well to complete the material and therefore do not see as much value in working in groups as the students who have not started. What they do see value in is further engagement in the content, particularly through the diversity of how information is presented to them.

Most students felt engaged by the lessons, which lead to most of them feeling motivated to finish / continue the lesson they were on. However not all, which is why additional techniques need to be attempted to engage more students. Comparing these results back to the very first survey where students were questioned about their experienced difficulty, we were able to flip the results and instead of the majority of students indicating



they experienced a 4/5 difficulty, they experienced a 4/5 in terms of engagement, motivation and understanding. Overall P4 was not developed to its fullest in *Unconventional Cryptography*, but still had visible success. Reassuringly, students identified room for improvement in the project to be what was lacking from a fully realised P4 principle, suggesting that P4 does lead to a higher engaged and better taught cohort of students.

Chapter 8

Future Work

For the lesson quality to improve and to engage more students, lessons should be open to accepting contributions. Using a collaboration and version control platform like GitHub, collaborators can add and change lessons, which can then be merged into the final resource after review. My time and motivation is a finite resource, allowing others to contribute would accelerate the development of the lessons. Additionally, the open source approach to lesson development introduces different perspectives into the lesson, better reaching a wider range of students, this will help combat the "Similar to me" bias which was recognised in the existing lessons of *Unconventional Cryptography.*

A large barrier for students using the resource is the requirement to make an Open-Learning account and sign up to the course. Some students would prefer to preview the course material before committing, others had concerns about the privacy of their personal data. From my experience running the course, student collaboration is never guaranteed, it requires a suitable environment and a critical mass of students. Collaboration however is a key principle that should be actualised to enhance a cryptography course, therefore a different platform also should facilitate this. What I would like to try is to host the content independently and then cultivate collaboration and a community through a study group where students can chat and help each other.

Unconventional Cryptography, is still somewhat conventional when it comes to the medium in which it communicates the content. Being an online site means that it is able to adopt videos, animations and other forms of multimedia to teach students. Due to time restrictions, these avenues were unable to be explored. For future work, these forms of communication should be experimented with to assess their effectiveness in educating students. From the student survey several students mentioned that videos, animations and interactive elements would be desirable in an online course, it was also the most requested aspect which students indicated would increase their motivation to continue with the course, therefore this idea should be explored further.

This research focused primarily on qualitative data to explore the field of cryptology education. While I have gained a greater insight into the student learning experience I am unable to make conclusive claims about the hypotheses. Further work on this subject should employ rigorous experimentation with quantitative data collection to try and accurately measure the existent (or non-existent) educational benefits of teaching cryptography according to my (and others) principles.

Chapter 9

Personal Development

Over the course of this project not only did I develop my cryptography skills but also gained an appreciation for conducting research, writing reports and promoting content. The thing I struggled with the most in this project was dealing with criticism. It's very easy to associate criticism of your work with criticism of yourself. I believe I experience this significantly because I try to embed part of my personality into the work I do. I learnt quickly that becoming defensive while reading negative comments was not productive towards improving the student experience. Part of my learning this semester was to not let my emotions regarding criticism dictate my response, instead, I need to analyse the feedback and attempt to understand the situation from the students point of view.

I am the easiest person to fool when thinking about the successfulness of my work, It's important that I stay conscious of this bias and correct it in order to discover the truth.

Chapter 10

Conclusion

From analysing student feedback to an empirical study of cryptography education, almost all students recognise the learning benefits of being taught cryptanalysis (P1) and completing practical programming exercises (P2). Most students reported learning the majority of the content from the lessons despite not being completely confident with their mathematics skills (P3). The selection of topics students attempted was limited and therefore we are unable to ascertain whether abstaining from using mathematics will continue to be effective in teaching cryptography. There is evidence to suggest the more mathematically mature a student is, the greater ease they will have in understanding cryptography, but using diverse set of mediums to explain content makes cryptography more accessible to computing students who tend to be mathematically immature. So the answer to the question ”Do you spend time teaching these students the prerequisite mathematics? Or do you try to teach cryptography using non-mathematical concepts?” is, do both; We have seen how both perspectives help students understanding of cryptography, and how each perspective has their advantages. To better teach cryptography to computing students, and to prepare them for learning more advanced mathematically oriented cryptography topics, a combination of both teaching styles is required. Lastly we have seen how creating emotionally engaging content does motivate students to continue their learning, but it’s easy to forget about the ”Similar to me” bias, and write content which engages only students that are similar to the educator. For self motivated students, community is less important, what they prefer is diverse engaging content that will keep them wanting to learn. For students who may struggle to find the motivation to begin, community was important to them, and could lead to a more engaged and motivated cohort.

Overall, there is evidence which suggests adopting my four principles in a cryptography educational resource will lead to high level of engagement and learning for computing students. Certain principles I did not follow through to their fullest potential, and as a result was unable to effectively motivate and teach certain types of students. However, the students recognised the same flaws I did and noted how their learning might be enhanced if P3 and P4 were executed to their fullest potential. The final thing to note is that no matter how effective your teaching resource might be, if no students are motivated to start going through the content, then it is not effective in helping anyone. Therefore out of all the principles, P4 is the most important as mastering it unlocks the opportunity to reach more students, especially those who feel underprepared and overwhelmed at the prospect of learning something new.

Appendix A

Cryptology education survey

See the attached AppendixA.csv document for the full spreadsheet of survey responses.

Line 13 in the sheet:

2018/03/09 3:45:42 PM GMT+11	No	Hello	Cameron	Nice	Survey

was discounted from the analysis as this was deemed a non-serious response.

Appendix B

Cryptography Course Survey

Course Name	Institution	Department	Assessment
Design and Analysis of Cryptographic Protocols	NYU	Computer Science	Theory Questions
Cryptography and Data Security	UMBC	Computer Science	Theory and Programming Questions
Computer and Network Security	MIT	Computer Science	Theory and Programming Questions
Cryptography and Computer Network-Security	George Manson	Computer Science	Theory and Programming Questions
Introduction to Cryptography	Clemson	Mathematics	Theory Questions
Cryptography	Princeton	Computer Science	Theory Questions
Cryptography	Purdue	Computer Science	Theory Questions
Cryptography	UC-Davis	Computer Science	Mostly Theory Questions
Introduction to Cryptography and Communication Security	Worcester Polytechnic Institute	Computer Science	Theory and Programming Questions
Cryptography and Information Security	California State	Computer Science	Theory and Programming Questions
Intro to Cryptography	Oregon State	Computer Science	Theory and Programming Questions
Introduction to Cryptography	Rochester University	Computer Science	Theory and Programming Questions
Information, Codes and Ciphers	University of New South Wales	Mathematics	Theory Questions
Computer & Network Security	University of Sydney	Computer Science (Engineering and IT)	Theory and Programming Questions

Appendix C

Interview ommitted for public release

Appendix D

Practical Cryptography Feedback

D.1 Reception to presentation and lesson clarity

D.1.1 Positive

http://practicalcryptography.com/ciphers/classical-era/affine/#comment-842931495

http://practicalcryptography.com/ciphers/classical-era/affine/#comment-3585063145

http://practicalcryptography.com/ciphers/classical-era/affine/#comment-1957910856

http://practicalcryptography.com/ciphers/classical-era/playfair/#comment-697550561

http://practicalcryptography.com/ciphers/classical-era/playfair/#comment-645966967

http://practicalcryptography.com/ciphers/mechanical-era/enigma/#comment-2303587566

http://practicalcryptography.com/ciphers/mechanical-era/enigma/#comment-913517553

http://practicalcryptography.com/miscellaneous/machine-learning/guide-principal-component-analysis-pca/#comment-3275403039

http://practicalcryptography.com/miscellaneous/machine-learning/tutorial-cepstrum-and-lpccs/#comment-3481786852

http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher-part-2/#comment-1685102905

http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/#comment-1922981418

http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/#comment-986358408

D.1.2 Negative

http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-bifid-cipher/#comment-1470989448

D.2 Mathematical symbols are a barrier to understanding

http://practicalcryptography.com/ciphers/classical-era/affine/#comment-2246656185

D.3 Author suggests mathematical maturity is essential for mastering cryptography

http://practicalcryptography.com/ciphers/classical-era/atbash-cipher/#comment-2247435883
http://practicalcryptography.com/ciphers/classical-era/atbash-cipher/#comment-2247729362

D.4 Reception of the content

D.4.1 Positive

http://practicalcryptography.com/ciphers/classical-era/rail-fence/#comment-726855308
http://practicalcryptography.com/ciphers/classical-era/rail-fence/#comment-607646635
http://practicalcryptography.com/ciphers/classical-era/columnar-transposition/#comment-2000379919
http://practicalcryptography.com/ciphers/classical-era/columnar-transposition/#comment-646614469
http://practicalcryptography.com/ciphers/classical-era/columnar-transposition/#comment-719931723
http://practicalcryptography.com/ciphers/classical-era/columnar-transposition/#comment-719933222

http://practicalcryptography.com/ciphers/classical-era/columnar-transposition/#comment-719932508

http://practicalcryptography.com/ciphers/classical-era/autokey/#comment-3663748832

http://practicalcryptography.com/ciphers/classical-era/beaufort/#comment-903392860

http://practicalcryptography.com/ciphers/classical-era/vigenere-gronsfeld-and-autokey/#comment-3669055417

http://practicalcryptography.com/ciphers/classical-era/vigenere-gronsfeld-and-autokey/#comment-1608547406

http://practicalcryptography.com/ciphers/classical-era/vigenere-gronsfeld-and-autokey/#comment-906842789

http://practicalcryptography.com/ciphers/classical-era/vigenere-gronsfeld-and-autokey/#comment-706196673

http://practicalcryptography.com/ciphers/classical-era/hill/#comment-639206074

http://practicalcryptography.com/ciphers/classical-era/playfair/#comment-1177337265

http://practicalcryptography.com/ciphers/classical-era/playfair/#comment-1153924823

http://practicalcryptography.com/ciphers/classical-era/playfair/#comment-706130378

http://practicalcryptography.com/ciphers/mechanical-era/enigma/#comment-2436638951

http://practicalcryptography.com/ciphers/mechanical-era/enigma/#comment-1134770529

http://practicalcryptography.com/ciphers/mechanical-era/enigma/#comment-988998507

http://practicalcryptography.com/ciphers/mechanical-era/enigma/#comment-800542622

http://practicalcryptography.com/miscellaneous/machine-learning/tutorial-cepstrum-and-lpccs/#comment-3295099832

http://practicalcryptography.com/miscellaneous/machine-learning/tutorial-cepstrum-and-lpccs/#comment-2316272613

http://practicalcryptography.com/miscellaneous/machine-learning/tutorial-automatic-language-identification-ngram-b/#comment-3384650161

http://practicalcryptography.com/ciphers/classical-era/atbash-cipher/#comment-2945911192

http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/#comment-3794642900

http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/#comment-3794638826

D.4.2 Negative

http://practicalcryptography.com/ciphers/classical-era/rail-fence/#comment-1244714367

Appendix E

Cryptopals Feedback

E.1 Not enough information

https://arstechnica.com/civis/viewtopic.php?p=33336507#p33336507

https://arstechnica.com/civis/viewtopic.php?p=33384221#p33384221

https://arstechnica.com/civis/viewtopic.php?p=33385115#p33385115

E.2 Positive Learning experience

https://news.ycombinator.com/item?id=12721708

https://arstechnica.com/civis/viewtopic.php?p=33744505#p33744505

https://news.ycombinator.com/item?id=12721623

https://news.ycombinator.com/item?id=12722495

E.3 Unmotivated

https://www.reddit.com/r/crypto/comments/5ktxg5/cryptopals_challenge_anyone/

E.4 Working together

https://groups.io/g/cryptopals8studygroup

http://lists.lrug.org/pipermail/chat-lrug.org/2014-September/010465.html

Appendix F

Serious Cryptography Feedback

https://www.goodreads.com/book/show/36265193-serious-cryptography

https://www.amazon.com.au/Serious-Cryptography-Jean-Philippe-Aumasson/dp/1593278268

Appendix G

Handbook of Applied Cryptography

https://www.quora.com/What-can-I-do-now-to-prepare-myself-for-a-job-as-cryptographer
in-the-future/answer/Bakhtiyar-Farayev

https://www.quora.com/What-are-some-good-resources-for-learning-about-cryptography/answer/Ryan-Lackey

https://www.reddit.com/r/crypto/comments/5mainf/i_want_to_learn_cryptography/dc2q5uc/

https://www.cybrary.it/0p3n/best-courses-e-books-learn-cryptography-beginners/

https://www.comparitech.com/blog/information-security/cryptography-guide/

https://security.stackexchange.com/a/5675

Appendix H

Unconventional Cryptography: Students feedback

See the attached AppendixH.csv document for the full spreadsheet of survey responses.

Bibliography

[1] Anatoly Temkin. Teaching cryptography to continuing education students. In *Fifth World Conference on Information Security Education*, pages 121–128. Springer, 2007.

[2] Bruce Schneier. The security mindset. Schneier on Security, 2008.

[3] Martin Mink and Rainer Greifeneder. Evaluation of the offensive approach in information security education. In *IFIP International Information Security Conference*, pages 203–214. Springer, 2010.

[4] William Yurcik and David Doss. Different approaches in the teaching of information systems security. 11 2001.

[5] Sara Hooshangi, Richard Weiss, and Justin Cappos. Can the security mindset make students better testers? pages 404–409, 02 2015.

[6] Ronald S Cheung, Joseph P Cohen, Henry Z Lo, and Fabio Elia. Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2011.

[7] Eman Sa. Incorporating hacking projects in computer and information security education: an empirical study. 6:185 – 203, 01 2014.

[8] Alexandros Papanikolaou, Vassilios Karakoidas, Vasileios Vlachos, Andreas Venieris, Christos Ilioudis, and Georgios Zouganelis. A hacker's perspective on educating future security experts. pages 68–72, 09 2011.

[9] Zouheir Trabelsi and Walid Ibrahim. Teaching ethical hacking in information security curriculum: A case study. pages 130–137, 03 2013.

[10] Neal Koblitz. Cryptography as a teaching tool. *Cryptologia*, 21(4):317–326, 1997.

[11] D D Leonard and G C Hamey. Teaching secure communication protocols using a game representation. 2003.

[12] Xavier Bultel, Jannik Dreier, Pascal Lafourcade, and Malika More. How to explain modern security concepts to your children. *Cryptologia*, 41(5):422–447, 2017.

[13] Timothy Bell, Harold Thimbleby, Mike Fellows, Ian Witten, and Neil Koblitz. Explaining cryptographic systems to the general public. 06 1999.

[14] Joshua Holden. A comparison of cryptography courses. *Cryptologia*, 28(2):97–111, 2004.

[15] Wm Conklin. The design of an information security practicum course. 01 2007.

[16] Cindy York and Jennifer Richardson. Interpersonal interaction in online learning: Experienced online instructors' perceptions of influencing factors. 16:83–98, 06 2012.

[17] D. Randy Garrison, Terry Anderson, and Walter Archer. Critical inquiry in a text-based environment: Computer conferencing in higher education. 2000.

[18] Chih-Hsiung Tu and Marina Mcisaac. The relationship of social presence and interaction in online classes. 16:131–150, 09 2002.

[19] J Lyons. Practical cryptography. 2009. URL http://practicalcryptography.com/.

[20] Devlin S Balducci A, Ptacek T and Wielgoszewski M. Cryptopals. 2012. URL https://cryptopals.com/.

[21] Paul R Pintrich. The role of motivation in promoting and sustaining self-regulated learning. *International Journal of Educational Research*, 31(6):459 – 470, 1999. ISSN 0883-0355.

[22] J.P. Aumasson. *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press, 2017. ISBN 9781593278823. URL https://books.google.com.au/books?id=hLcrDwAAQBAJ.

[23] D Boneh. Cryptoraphy i. 2018. URL https://www.coursera.org/learn/crypto.

[24] F Valsorda. Live streaming cryptopals. 2017. URL https://blog.filippo.io/live-streaming-cryptopals/.

[25] A.J. Menezes, J. Katz, P.C. van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 1996. ISBN 9781439821916. URL https://books.google.com.au/books?id=MhvcBQAAQBAJ.

[26] John Morkes and Jakob Nielsen. Concise, scannable, and objective: How to write for the web. 05 1997.

[27] Paul Ginns, Andrew Martin, and Herb Marsh. Designing instructional text in a conversational style: A meta-analysis. 25:445–472, 11 2013.