An Exploration of Cryptography

Internation School of Helsinki

Siddharth Mahendraker
siddharth_mahen@me.com

Word Count: 2500

2012

Contents

The Goal

The realm of computer science has captivated me since my youth. It has always been an interest of mine which I have persued inside and outside of school. These days, I continue to write programs in my spare time, publish open source software, and contribute to other open source projects over the Internet.

Therefore, when the time came to pick a topic for my personal project, a topic in the field of computer science seemed like an obvious choice.

Through my own interest, I had already taken time to learn about many of the interesting subtopics in computer science, such as computational complexity theory, artificial intelligence, algorithm and data structure design and software engineering. As such, I wanted to try something a little different; something new and challeging.

I chose to learn about cryptography because it was a field of computer science I genuinely knew nothing about, yet contained so many intersting ideas. What really drew me in was the fundamental problem that cryptography solved: it allowed people to communicate securly over completely insecure channels. I was really interested in learning about the mathematical theory underneath cryptography and how it could be implemented in the real world.

I think the area of interaction to which cryptography most relates is human ingenuity. This is because cryptography (and for that matter any field in computer science) is based on inventing creative concrete solutions to abstract problems. In cryptography, these solutions take the form of cryptographic alorithms and their implementations and these problemes take the form of mathematical equations.

Based on my area of interaction and my interests, human ingenuity and learning about both applied and theoretical cryptography respectively, I came up with the following inquiry question: ”What ingenious ideas and processes are involved in modern cryptographic theory, and how do they function in practice?”.

I decided that the best way to achieve my goal and answer my inquiry question was to write three seperate cryptographic algorithms embodying my research and then compare and constrast these algorithms in a research report. This goal is particularly well suited to my needs as it balances both the applied and the theoretical parts of cryptography, allowing me to focus

on the entire subject as a whole.

Idealy, my product should follow the following specifications.

Firstly, it should be deep and complete. In my mind this means simple, intuitive explanations and worked examples. Around 20-30 pages would be sufficient, perhaps.

Secondly, it should include a mix of theory and real life applications. As my inquiry question states, this is as much about practice as it is theory.

Thirdly, it should provide code examples. Personally, I hate reading computer science related studies unless I can verify the code myself. If I am going to write something, it had better have code so my readers can check the validity of my work.

Lastly, it should look good and be entertaining to read. If I am going to write about a topic that I spent a whole year researching, the paper I submit should convey some of my passion for the subject and be pleasant to look at.

Selection of Sources

My research spanned a wide variety of subjects in both theoretical and practical cryptography.

One of the most useful books I have used is Applied Cryptography by Bruce Schneier [2]. It gave me invaluable information into the practical application of cryptography with solid definitions, great bredth and full code examples. I was sure this book was a good resource because the author, Bruce Schneier, is a very well known security technologist, who currently serves on the board of directors of the International Association of Cryptologic Research and is a member of the Advisory Board for the Electronic Privacy Information Center while also working at a consulting firm specializing in cryptography and computer security. Furthermore, he has also designed one of the strongest block ciphers currently available, called `bcrypt`. I found this book by asking about good introductory texts to cryptography on Quora.

The next invaluable resource I used was An Introduction to Mathematical Cryptography by Joseph H. Silverman et ali [1]. This book gave me a complete and through understanding of the underlying mathematics behind

a wide variety of cryptographic algorithms, as well as insight into interesting mathematical techniques which could be used to break these algorithms. The book was initially an extremly tough read, as I was not used to its rigorous proof based method. However, with practice and much time spent on the wonderful examples at the end of each chapter, I was able to use this book effectively. All of the authors of this book are proffessors of mathematics are Brown University, and have all published numerous research articles in their respective fields of mathematics, therefore I beleive that this book contains trustworthy information.

Another huge resource which I took advantage of was websites such as Khan Academy and Wikibooks. Khan Academy creates and distributes short Youtube videos explaining topics in a wide variety of disciplines. Wikibooks provides free, detailed texts regarding a wide variety of subjects. Although these resources were not used when looking for information regarding topics in cryptography (as, in the case of Wikibooks, anyone can become an author), they were extremely useful when I wanted to review certain topics, such as binomial coefficients or how to use the typesetting software (LaTeX), properly.

Aside from these resources, I have also referred to a many different individual articles from various online sources, ranging from an article on elliptic curve cryptography form the NSA to articles from Wolfram Alpha about the applications of cellular automata in cryptography.

When it came to picking my resources, I opted for quality over quantity. Although I did not choose an enourmous selection of resources as some students have, the resources I did choose were of excellent quality and were ultra dense in information. For example, both of the books mentioned above are well over 450 pages in length (501 and 758 pages respectively).

Application of Information

Over the course of my project, there were a slew of skills and techniques I developed as a result of my research, which concentrated themselves in two main categories.

Firstly, and perhaps most importantly, I learned about the actual processes involved in the use and the construction of cryptographic systems. I learned about techniques such as statistical analysis of text, linear cryptanalysis

and the analysis of elliptic curve discrete logarithm based cryptosystems, just to name a few. These techniques were applied directly to my product in two distinct ways. Firstly, all of these ideas were explained in detail, with worked examples. This should demonstrate my ability to apply this information through my ability to teach it to others. Secondly, I have written programs for both the encryption and the cracking of each of the algorithms in my product. This should further demonstrate my understanding of the subject.

Secondly, I learned to apply many auxiliary skills to acheive my project goals. These skills were not central to answering my inquiry question, but rather served to enchance and improve my project as a whole. One of the most important example of this was my development of my ability to read and understand mathematical texts. At the beginning of the project, I had absolutely no idea how to read mathematics, which resulted in me flipping back between pages trying to understand what was happening during a proof or when building on a previous topic. As the project progressed, I learned to read carefully and use my resources properly (for example, by doing the questions at the end of each chapter, or working all of the examples by hand). Furthermore, apart from helping me understand the texts I was reading, this helped me structure my writing style appropriately, so I sound clear and professional throughout my research report. Another great example of the skills I learned to apply are my new found LaTeX typsetting skills. Before this project began, I had not even heard of LaTeX, but after doing some research on better typesetting engines (Microsoft Word does not set mathematical text very well...) I chanced upon LaTeX and took it upon myself to learn how to use it. The wonderful Wikibook on LaTeX provided me with everything I needed to know. Using this knowledge, I constructed not only my product, but also this essay.

I realize this may sound haughty, but I trully feel that anyone who is to grade me on my application of information should really read my product to truly understand the extent to which I have applied the information I learned. This being a reflective essay, the technical content of my project has only been vaguely mentioned (as above). However, in reality, my depth and application of knowledge is quite quite substantial and I think this should be taken into consideration. Here is a brief example of my application of such technical information: Early on in the project, I was having trouble understanding why Shank's baby step giant step collision algorithm for the discrete logarithm problem, $g^x = h$, required lists of size slightly larger than the size of the square root of the order of the element g. It seemed absolutely strange at first, however, as I continued through

the book, I learned about the Collision Theorem and how it (practically) guarantees that you only need to check a small multiple of the size of the square root of the list before you find a match, because by that point the probability of not finding a match is very very low.

Achieving the Goal

My goal was to answer the question "What ingenious ideas and processes are involved in modern cryptographic theory, and how do they function in practice?", and I think that I have succeded in acheiving that goal with regard to my product.

My research report meets almost all of the specifications I set out to acheive. It is deep and complete, with lots of examples and many simple yet detailed explanations. It focuses on both the practical and theoretical sides of cryptography. It gives full code examples of all of the cryptographic algorithms analyzed, as well as several extra programs which were used in the analysis of these algorithms. And finally, it has been beautifully set using LaTeX, and includes gorgeous tables and exquisite mathematical typesetting.

Although I cannot vouche for how pleasant my report is to read, being the author, I do beleive it flows quite nicely, and although far from being professionaly written, conveys my passion and interest in the subject.

Based on all of the above, I would give myself a level 4.

I think the two main criteria which define the success of this project is the meeting of the first and second specifications. The other two are simply more personal goals which are not directly related to my inquiry question or the topic of my project.

Reflecting on Learning

Throughout my project, my learning was divided into two main categories.

The first, and largest category, was dedicated to my learning of cryptography. I learned about a myriad of topics ranging from the construction and

analysis of cryptographic algorithms to number theory. During this learning, I was learned to hone my mathematical and programmatical skills. One of the most important improvements in my mathematical skill was my ability to read mathematical texts properly and understand the material. At the beginning of the my project, I was reading dense mathematics as though it were a novel. I soon realized that truly understanding mathematical texts involves reading, re-reading, analyzing and working through examples. I learned not only to understand the authors conclusions, but also what lead them to those conlusions, and how their proof is applied in the context of the problem. From this, I learned how I should be constructing my proofs and logical reasoning, and how to imitate the style these authors used in my own research report.

The second category was about intrapersonal learning. This project really pushed the limits of my perseverance and my patience. Sometimes, I would stare at my textbook for a good 45 minutes, pulling my hair out trying to figure out why the math worked the way it did. Sometimes, I would have to work 15 or more problems from the back of the book before I understood the real implications of what was going on. I learned to know when I was in the mood to understand something, and when I was wasting my time hitting my head against the wall. I also realized the importance of occasional breaks, despite tight deadlines, which always helped me clear my mind and focus on the task at hand.

All of this has significantly improved my self direction as a learner.

As this project project progressed, I came to a very profound conclusion regarding cryptography, mathematics and the nature of human ingenuity. I realized that simply by making up structure, and imagining new possiblities, humans have the capacity to reveal deep truths about our universe. And in that respect, human acheivement is only limited by out imaginations. Although this idea seems trivially simple, it has changed the way I think about science, innovation and especially, mathematics. I have come to seethe intrinsic beauty of mathematical structure, and its ability to reveal amazing and wonderful truths through the sheer power of imagination.

If I were to do a similar project in the future, I would improve my management of time by allocating more of it towards writing the research report and less of it towards doing research. Although thourough research was crucial to the success of my product, I felt as though I could progressed through my research report with less stress had I started working on it earlier. This would have also allowed me to have more time to edit and

refine my work, which is always appreciated. I think I could acheive this next time by allocating work more granularly, rather than in large chunks. This way, I would be able to stop and asses myself more often, so that I can makes changes in my plan earlier in the process. For example, during this project, I allocated work in month based chunks, meaning all of my work was due at the end of the month. Rather than do this, I should have allocated work in week based chunks, so that my goals wouldn't seem as large and I would be able to make more ammendments to my plan as the project progressed.

All in all, I am really glad I did this project. I have really taken my abilities to their full potential. I learned an incredible amount, not only about cryptography, but also about myself.

Bibliography

[1] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, 233 Spring Street, New York, N.Y., USA, 2008.

[2] Bruce Schneier. *Applied Cryptography*. John Wiley and Sons, Inc., 605 Third Avenue, New York, N.Y., USA, second edition, 1996.