An Exploration of Cryptography

Internation School of Helsinki

Siddharth Mahendraker
siddharth_mahen@me.com

Word Count: 820

2012

Contents

0.1 The Goal 1
0.2 Selection of Sources 2
0.3 Application of Information 3
0.4 Achieving the Goal 5
0.5 Reflecting on Learning 6

0.1 The Goal

I have always been interested in computer sciences. It has captivated me since my youth, and to this day, I continue to write programs, publish open source software, and contribute to others' work.

Therefore, when the time came to pick a topic for my personal project, computer sciences seemed like the obvious choice.

My almost insatisfiable craving for computer science related knowledge has led me down several very interesting paths. I have previously taken my own time to learn about topic such as fundamental computation theory, artificial intelligence, algorithm and data structure theory and software engineering. However, computer science still holds many wonders for me to discover, and cryptography was one of them.

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, 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, the research report 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.

0.2 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[1]. 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 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 is An Introduction to Mathematical Cryptography by Joseph H. Silverman et al[2]. This book gave me a complete and through understanding of the underlying mathematics behind a wide variety of crpytographic algorithms, as well as insight into intersting mathematical techniques which could be used to break these algorithms.

The book was initial an extremly tough read, as I was not used to it's 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 have used regularly is Khan Academy. It's a sort of online learning resource which teaches you subjects in small YouTube clips in less than 10 minutes. This was particularly useful if I wanted to review something such as matrix multiplication, if I hadn't done it in a while. Just to brush up my math skills in general.

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 chose an enourmous selection of resources as some students have, the resources I have chosen are of excellent quality and are ultra dense in information and each entry in my bibliography has been thoroughly vetted.

0.3 Application of Information

Because I knew absolutely nothing about cryptography before I began, many of my first problems involved simply not understanding what was going on. The solution, although it may seem slightly stupid, was simply to study my resources very carefully and ensure I understood the concepts presented.

For example, 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

[1] Applied Cryptography - Protocols, Algorithms and Source Code in C by Bruce Schneier

[2] An Introduction to Mathematical Cryptography by Jeffery Hoffstein, Jill Pipher and Joseph H. Silverman

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.

Later in the project, my resources also helped me make desicions for which there was no mathematical or logical reasoning. For example

Based on my research, I had already decided I would be investigating symmetric and public key cryptography because it was the basis for other more complex areas in cryptography such as visual cryptography, quantum cryptography and cryptographic hashing, which I personally really wanted to learn about outside the context of this project.

However, I still had not decided which cryptographic algorithms (hereafter referred to as ciphers) to write about. I wanted to cover a large spectrum of symmetric and public key cryptography to demonstrate my knowledge of the topic, while simoultaneously

The first and most important instance where my research came into play was when I had to choose which subtopic of cryptography to write in my product. Cryptography is a very, very diverse field, with many highly interesting subtopics, including several which really caught my eye such as homomorphic cryptography, quantum cryptography and cryptographic hashing.

After the first month of two of research, I realized something important, which in hindsight, I really should have forseen earlier. The bredth of the subject would be impossible to capture with my skills and my time constraints. The problem was all of the subtopic in cryptography were

I would have to choose a particular subtopic in cryptography

My project was completed in 2 phases, research and the writing of my report.

The first phase, research, was the longest and most difficult phase. During this time, I was constantly researching new and interesting things about the realm of cryptography. I began at the basics, the information theoretic foundation of cryptography, its assumptions and its underlying ideas. Then I began researching different sub-ideas in cryptography, such as mathematically difficult algorithms, probability theory, number theory and crpytographic protocols. After every research session, I would consiously not look into one topic I found very interesting so that next time I would know right where to start off.

Soon however, I realized that the huge bredth of the subject was impossible to capture with my skills and my time constraints. Therefore, of the research I had done, I looked at only a small subset of that. I choose cryptographic ciphers and their implementation because it was very interesting, it was within my ability to program such programs and they came in a variety of difficulties so I could really show off my skills in the product. Furthermore, it was a subset of cryptography that was relatable to other people, and has very strong connections to my area of interaction.

Then I began my second phase, the writing of the report. Because I had already researched everything I needed to know, the content of the research report came fairly naturally. What took the longest amount of time was structuring what I knew into a text that made sense and flowed smoothly from one idea to the next without doing any magic. That is, I wanted to give the reader a real understanding of what is going on, rather than just an answer. This was acheived simply by writing extensively at every oppertunity. Slowly, I carved my final paper out of the giant mess of attempts.

Note, however, that there are a myriad of other interesting topics in the field of cryptography (such as cryptograhic hashing, homomorphic cryptography, visual cryptography, quantum crpytography etc...) which are equally interesting, but I sadly could not include in my project.

0.4 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.

0.5 Reflecting on Learning

Although I learned an incredible amount about crytography while investigating and making my product

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.

Although I learned about fantastic and beautiful ideas such as those involved in information theory, probability theory, crpytographic analysis of algorithms, number theroy, the construction of cryptographically secure algorithms and other such technical topics. I felt as though the true learning

Reflecting on my endevours through the lens of Human Ingenuity has provided a very interesting insight. As this project progressed, I came to a very profound conclusion regarding cryptography, mathematics and the nature of human innovation. I realized that simply by making up structure, and imagining new possiblities, humans have the capacity to reveal deeper truths about our universe. And in that respect, human acheivement is only limited by our imaginations. And although this idea seems trivially simple, it has truly changed the way I think about science and innovation, and especially mathematics. I have come to see the intrinsic beauty of mathematical structure, and its ability to reveal amazing and wonderful things through the sheer power of imagination. Things such as Diffie-Hellman key exchange continue to amaze me. The very idea that such a structure preserves information withouth any prior secrecy is astounding.

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. Although the its outcome was important, I feel the real gain has been in my self confidence and my ability to persevere and deliver results. I now know myself better, and I can make more accurate judgements regarding my strengths and my weaknesses.

All in all, I am really glad I did this project. Not only have I learned an incredible amount about cryptography, but I have also developed my self-awareness, perseverance and ability to solve challenging problems.