An Exploration of Cryptography

Internation School of Helsinki

Siddharth Mahendraker
siddharth_mahen@me.com

Word Count: 820

2012

Contents

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.

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 in-

[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

dividual 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

0.4 Achieving the Goal

0.5 Reflecting on Learning