I have not decided this yet

BY

Weiqi Feng

A Study

Presented to the Faculty

of

Wheaton College

in Partial Fulfillment of the Requirements

for

Graduation with Departmental Honors

in Mathematics

Norton, Massachusetts

May 2019

Acknowledgments

Contents

Abstract

I need two to three sentences here talking about this thesis.

Chapter 1

Introduction

In this chapter, we introduce the definition of cryptography. We talk about what cryptography used to be and what it is in the modern times. Then we move on to discuss how Rubik's Cubes and cryptogrpahy can be closely related. Finally, we introduce some important preliminaries that we will use through this thesis.

1.1 What is cryptography

The definition of cryptography given in the Webster dictionary is "*secret writing*". This is historically precise. In ancient times, people apply the idea of cryptography solely to enable secret communication. Most ancient cryptography schema, as well as some modern ones look like some kind of puzzle. Yet creating and breaking the schema would reply on how well you can manipulate the puzzle. Substitution cipher can be considered as a monumental example of such type. Based on its name, we have a good intuition on what substitution cipher does. That is, replace each unit of the plaintext (e.g. each letter in one English sentence.) to a ciphertext. And such correspondance between plaintext and ciphertext can be very creative. Clearly, the more abstract the substitution is, the less chance people who don't know the substitution method can break the ciphertext. Also, the biggest motivation for people to research in this field and in fact, most applications of this field were military related. Thus the term cryptography seemed far away from people's daily life.

However, cryptography has largely changed since the invention of computers and the internet. It has merged deeply into our daily life though you may not have noticed. Every time when you log in your email account or when you purchase an item from an online shop, you have undoubtedly used cryptography. While we cannot deny securing communication is still a major functionality of cryptography, the study of cryptography has developed other branches that are just equally important. Some of the noticeable branches that modern cryptography involves are key exchanging protocols, message authentication methods, hash functions and etc. One of the other thing computers brought to us is the ample computational powers. In present, a 30 dollars Raspberry Pi can do an exhaustive attack on the substituion cipher on 26 English letters in just the time of making a cup of coffee. Thus, deriveating from studying the art of clever puzzles, modern cryptography makes extensive use of mathematics, including fields such as abstract algebra, number theory, statistics, combinatorics and computational complexities. And thus, modern cryptogrpahy protocols are designed around some computational hardness assumptions.

In a nutshell, cryptography has gone from the set of clever puzzles concerned with ensuring secret communication for the military to a science that provides security for ordinary people across the globe.

1.2 Rubik's cube and cryptography

Rubik's cube is a three dimensional puzzle invented in 1974 by Hungarian professor Ernő Rubik. As shown in Figure 1.1, the most common rubik's cube has six faces. The faces of the cube are covered by the following solid colors: white, red, blue, yellow, orange and green. For a solved cube, the white face is always opposite to the yellow face, red is opposite to orange and blue is opposite to green. In Figure 1.1, the rubik's cube has three small cube on each side. We say that this rubik's cube is a 3 by 3 by 3 one. And clearly each face of the cube includes nine smaller cubes. In future discuss, we will call those small cubes cubies. After years of developing, rubik's cubes now exist in tons of different forms. For the ones that have six sides, they can differ on their side lengths. And the side length varies from 2 to 13 or even larger numbers. And rubik's cubes are not no longer required to be a cube anymore. We also have seen rubik's cubes with four side or twelve sides.

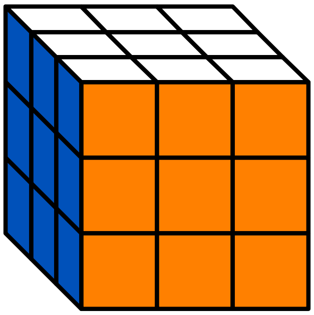

Figure 1.1: A rubik's cube at the solved state.

Why would we relate rubik's cubes and cryptography? Obviously, rubik's cubes provide a good shuffling schema. And rubik's cubes are known to be hard to solve. One may argue that this is not true, since the best human players can solve a 3 by 3 by 3 cube in about 6 seconds. Also by following the developed algorithms, anyone can solve a well shuffled rubik's cube on a scale of minutes. However, it is true that rubik's cubes have a lot of different states. The most common 3 by 3 by 3 rubik's cube have over 43 quintillion different states. It will take hundreds of years for a powerful desktop to run through all the possible states. Then we know that a schema designed based on rubik's cubes could be safe against exhaustive search attacks. In addition, we can view rubik's cubes as groups. The nice properties of groups are widely used in cryptography. We will explore more about this in the following chapters.

1.3 Preliminaries

First let's take a look at ***Kerckhoffs' principle***:

> *The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.*

This principle tells us that the security of one encryption protocol does not rely on the encryption protocol procedures being secret. So how do we obtain the security while the eavesdropper knows the encryption schema being used? (Talk about the key is secret. Talk about what Gen, Enc and Dec do. Talk about the correctness of encryption schema.)

Chapter 2

The group structure of the cube

A 3 by 3 by 3 cube has 6 fundamental moves. (Write out what they are.) Claim that rubik's cube in Figure 1.1 under its fundamental moves can be view as a group, in more details, a permutation group. Since essentially, what each movement of rubik's cube does is to send one cubie to another location. In order to illustrate this idea, we find a numbering system for it and we define the six fundamental moves as permutations.