

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

Acknowledgments	i
Abstract	iii
1 Introduction	1
1.1 What is cryptography	1
1.2 Rubik’s cube and cryptography	3
1.3 Preliminaries	4
2 The group structure of the cube	6

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 today. Moving forward, we discuss how Rubik's Cubes and cryptography can be closely related. At its conclusion, 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, since 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 rely on how well you can manipulate the puzzle. Substitution cipher, which replaces each unit of the plaintext to a ciphertext, can be considered as a significant example of puzzle like encryption. Intuitively, we know the security of substitution cipher is based on the fact that the correspondence between plaintext

and ciphertext is unknown to the attacker. Such correspondence can be very creative as long as the communicating parties hold the same information. Assume that we are working with English, in this case, unit of plaintext will be each letter. One trivial example could be substitute each letter to another unique letter like shown in Figure 1.1. Another creative example is shown in Figure 1.2, where we are replac-

A	B	C	D	E	...	Y	Z
↓	↓	↓	↓	↓	...	↓	↓
S	F	O	U	T	...	E	R

Figure 1.1: Map letter to letter.








A	B	C	D	E	...	Y	Z
↓	↓	↓	↓	↓	...	↓	↓
					...		

Figure 1.2: Map letter to icon.

ing letters by icons which are completely irrelevant. In general, we would say the more abstract the substitution is, the less likely for someone who doesn't know the correspondence to break the encryption schema.

What else worth mentioning is that, in history, 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 equally as important. Some of the noticeable branches that modern cryptography involves are key exchanging protocols, message authentication methods, hash functions and more.

One of the other thing computers brought to us is the ample computational powers. In modern times, a 30 dollars Raspberry Pi can do an exhaustive attack on the

substitution cipher on 26 English letters in the time it takes to make a cup of coffee. Thus, deviating 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. Modern cryptography 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, as shown in Figure 1.3, is a three dimensional puzzle invented in 1974 by Hungarian professor Ernő Rubik. 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 1.3, the rubik's

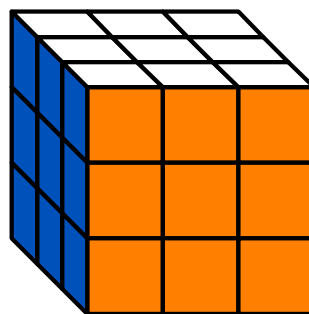


Figure 1.3: A rubik's cube at the solved state.

cube has three small cube on each side. We say that this is a 3 by 3 by 3 cube. 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 many forms. For the six

faced cubes, their side lengths may vary from 2 to 13 or even larger number cubies. However, since their structures are similar, they share a lot of properties in common. That is to say that no matter the side length, all six faced cubes can be solved in an almost identical fashion. Rubik's cubes also have other structures; "cubes" with four or twelve faces have also been made in production.

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. By following the developed algorithms, anyone can solve a well shuffled rubik's cube within minutes. Let's consider each different shuffling result of the rubik's cube as a state. It is true that rubik's cubes have a lot of different states. The most common 3 by 3 by 3 rubik's cube has over 43 quintillion different states. It will take hundreds of years for a powerful desktop to run through all of them. Being such a powerful device, 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 1.3 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.