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

The definition of cryptography given in the Webster dictionary is "secret writing." This definition is historically precise. In ancient times, people apply the idea of cryptography mainly to secure their communications. The biggest motivation to research in this field and in fact, most applications of this field were all military related. Thus

abstract The Concise Oxford English Dictionary defines cryptography as the art of writing or solving codes. This is historically accurate, but does not capture the current breadth of the field or its present-day scientific foundations. The definition focuses solely on the codes that have been used for centuries to en- able secret communication. But cryptography nowadays encompasses much more than this: it deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic auctions and elections, digital cash, and more. Without attempting to provide a com- plete characterization, we would say that modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks. The dictionary definition also refers to cryptography as an art. Until late in the 20th century cryptography was, indeed, largely an art. Constructing good codes, or breaking existing ones, relied on creativity and a developed sense of how codes work. There was little theory to rely on and, for a long time, no working definition of what constitutes a good code. Beginning in the 1970s and 1980s, this picture of cryptography radically changed. A rich theory began to emerge, enabling the rigorous study of cryptography as a science and a mathematical discipline. This perspective has, in turn, influenced how researchers think about the broader field of computer security. Another very important difference between classical cryptography (say, be- fore the 1980s) and modern cryptography relates to its adoption. Histor-

ically, the major consumers of cryptography were military organizations and governments. Today, cryptography is everywhere! If you have ever authenticated yourself by typing a password, purchased something by credit card over the Internet, or downloaded a verified update for your operating system, you have undoubtedly used cryptography. And, more and more, programmers with rel- atively little experience are being asked to secure the applications they write by incorporating cryptographic mechanisms. In short, cryptography has gone from a heuristic set of tools concerned with ensuring secret communication for the military to a science that helps secure systems for ordinary people all across the globe. This also means that cryptography has become a more central topic within computer science.