ROYAL HOLLOWAY, UNIVERSITY OF LONDON

Enigma: Prime Numbers and Cryptosystems

by

Adam Mulligan

A final year project submitted in partial fulfillment for the degree of Bachelor of Science, Computer Science

in the
Department of Computer Science

January 2012

"Anyone can design a security system that he cannot break. So when someone announces, Heres my security system, and I cant break it, your first reaction should be, Who are you? If hes someone who has broken dozens of similar systems, his system is worth looking at. If hes never broken anything, the chance is zero that it will be any good."

Bruce Schneier, *The Ethics of Vulnerability Research*

Abstract

Modern cryptography allows us to perform many types of information exchange over insecure channels. One of these tasks is to agree on a secret key over a channel where messages can be overheard. This is achieved by Diffe-Hellman protocol. Other tasks include public key and digital signature schemes; RSA key exchange can be used for them. These protocols are of great importance for bank networks.

Most such algorithms are based upon number theory, namely, the intractability of certain problems involving prime numbers. The project involves implementing basic routines for dealing with prime numbers and then building cryptographic applications using them.

Acknowledgements

With thanks to my project advisor Yuri Kalnishkan, and the RHUL Department of Computer Science for three years worth of knowledge and experience.

Contents

List of Figures

List of Tables

Abbreviations

AES **A**dvanced **E**ncryption **S**tandard

Chapter 1

Introduction

1.1 What it's about

Secrecy has always been of great importance, not just in modern society, but throughout history. Until very recently, Cryptography was consigned to the sending and receiving of messages, generally using pen and paper. However, increasingly cryptography – the study and implementation of techniques for secure communication[1] – is becoming more vital to the smooth running of even basic systems, whether it's the cliché example of military secrets or simply a micro-payment for an online service. Initially, the usage of provably secure and efficient cryptographic algorithms was limited to governments and related contractors, however the advent of encryption standards, and more relevantly, the creation of public-key cryptography mechanisms, has pushed it in to a wider field of use as researchers gained a better understanding of the area.

1.2 Goals and Intentions

The primary goal of this project can be found in the title and abstract: to research, discuss and create algorithms within or related to the field of prime numbers. To complete this task I will be developing my thoughts and discoveries regarding prime numbers as this report progresses, as well as producing a number of deliverables in the form of

[1] http://en.wikipedia.org/wiki/Cryptography

software applications, test results and statistics.The topic of number theory is in itself fascinating, and extraordinarily vast, however I will only be scratching the surface. Nonetheless, I hope to explain throughout this project how prime numbers have become such an important part of modern cryptography, and what they can be used for.

1.3 Project Summary

I will be splitting the project in to four main parts, excluding this report:

1. **Prime numbers in software**

   A discussion of how prime numbers can be efficiently produced programmatically, and software to prove it.

2. **Algorithms**

   The development of algorithms using prime numbers, such as RSA, and complementary cryptographic algorithms such as AES. Alongside this, the development of non-major algorithms in the field of prime number based cryptography that still present an academically interesting concept.

3. **Final Application**

   The production of a software program that utilises the implemented cryptographic algorithms in section 2 to display their efficacy in a real world application.

4. **Cryptanalysis**

   Taking the algorithms created and comparing them with official implementations for statistical analysis, alongside researching and performing "attacks" on them to prove or disprove the implementation's cryptographic security.

The primary algorithms to develop are:

- Asymmetric
  - RSA
  - Diffie-Hellman
- Symmetric

  - AES

- Identification and Authentication
  - RSA Signing
  - Digital Certificates

Other algorithms will be discussed and produced alongside these, however they will not be used in the final application testbed and are purely for research interest. These can be found listed in the contents in the relevant sections.

1.4 Other Information

This document was written and composed with LaTeXusing *Taco Software's Latexian*. The LaTeXsource code for this report should have come bundled with the project documentation and files, however if you are unable to retrieve it please see section 1.4.1.

1.4.1 Project Repository

If any part of this report is missing, you believe that you do not have a full access to the source code discussed in this document, or if any files have been lost, it is available for full download at `http://cyanoryx.com/files/project.zip` **(SHA-1 Sum:** `x`**).**

1.4.2 Openness

As with any field of study, the quality of research and development is dependent on the open distribution and sharing of ideas. This is *particularly* important with regards to cryptography. As said, cryptography was once reserved to government and research was conducted in secrecy. The open sharing of relevant information in this field is not just for the furthering of knowledge, but also to allow others to inspect and examine algorithms, a process that drastically improves the security of a system. As such, the entirety of this project is licensed under the **GNU General Public License version 3 or greater** and is available for access publicly online.

Chapter 2

Cryptographic Primitives

2.1 Basics of Information Security

Despite how it is portrayed or colloquially used, Information Security is an entirely different concept and area of study compared to Cryptography. It might seem simple enough to implement a basic cryptographic protocol involving encryption and decryption, however to introduce this into a system and expect the information to be secure, is foolhardy. Cryptography is a *means* to providing information security when following certain rules and guidelines not the be all, end all solution. An understanding of information security, and the related issues, is necessary.

This can be proven using historical evidence: throughout history many complex systems of mechanisms, rules, and protocols have been developed to introduce information security to a system. As with modern day security, this cannot be achieved entirely through mathematical and cryptographic means – it is more than just computational intractability.

As such, stringent criteria for developing secure systems and protocol have been introduced. While institutes such as *The British Computing Society* and *Association for Computing Machinery* ensure their members follow a professional code of ethics, just as a doctor might, these information security criteria are of separate and equal importance. Indeed, there are now several international organisations that exist solely for the overseeing of cryptographic research and development (See: *International Association for Cryptologic Research*).

Often, as we will see, cryptographic systems are simplified for the purposes of presentation particularly for textbooks. This will be discussed further later, with regards to the differences and difficulties involved in developing systems that do not just follow a mathematical "recipe," but also include information security values and other subtleties.

The overall method of dealing with, and ensuring, information security is known as risk management. This encapsulates a large number of countermeasures (including cryptography) that reduce the risk of vulnerabilities in, and threats to, systems. We will only be encountering and discussing the technological areas of mitigation, however some of the solutions include[1]: access control, security policy, physical security, and asset management.

2.2 Key Concepts and Objectives

As said, secure systems should follow a guideline, or set of criteria, that ensure the security and integrity of data stored and input. A clear and concise specification should be developed, that will aid the designer in selecting the correct cryptographic primitives, but also help the engineer implement the protocol correctly. There are many of these criteria, however each is derived from four primary objectives:

1. **Confidentiality** is the ability to keep . Maintaining confidentiality of data is an obligation to protect someone else's secret information if you have been entrusted with it.

[1]For an excellent resource regarding information security, both technical and non-technical, see *Security Engineering*, Ross Anderson

Chapter 3

Cryptographic Primitives

3.1 Cryptography Basics

3.2 Real Life Cryptography

3.3 Primitives

3.3.1 Key Agreement

3.3.2 Encryption

3.3.3 Authentication and Identification

3.3.4 Hashing

Chapter 4

Algorithm Implementations

4.1 Command Line Implementations

ffsdsfsd

4.2 Key Agreement

4.2.1 RSA

4.2.2 Diffie-Hellman

4.3 Encryption and Symmetric Ciphers

4.3.1 AES

4.3.2 Twofish

4.4 Authentication and Identification

4.4.1 RSA Signing

4.4.2 Digital Certificates

4.5 Hashing

4.6 SHA Family

4.7 Skein

sfdsfsdfsd

Chapter 5

Enigma: A Testbed

5.1 Description

5.2 Protocol

5.3 Interface

Chapter 6

Attacks and Flaws

????

Chapter 7

Further Research

????

Chapter 8

Enigma: A Testbed

8.1 Description

8.2 Protocol

8.3 Interface

Chapter 9

Attacks and Flaws

????

Chapter 10

Further Research

????

Appendix A

Enigma Application Specification

Write your Appendix content here.

Appendix B

Enigma Protocol Specification

Write your Appendix content here.