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

December 2011

"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

Chapter 2

Mathematical Basis

2.1 Number Theory

2.2 Prime Numbers

2.2.1 Finding Prime Numbers

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

????

Appendix A

Enigma Application Specification

Write your Appendix content here.

Appendix B

Enigma Protocol Specification

Write your Appendix content here.

Bibliography

[1] A. S. Arnold, J. S. Wilson, and M. G. Boshier. A simple extended-cavity diode laser. *Review of Scientific Instruments*, 69(3):1236–1239, March 1998. URL `http://link.aip.org/link/?RSI/69/1236/1`.

[2] Carl E. Wieman and Leo Hollberg. Using diode lasers for atomic physics. *Review of Scientific Instruments*, 62(1):1–20, January 1991. URL `http://link.aip.org/link/?RSI/62/1/1`.

[3] C. J. Hawthorn, K. P. Weber, and R. E. Scholten. Littrow configuration tunable external cavity diode laser with fixed direction output beam. *Review of Scientific Instruments*, 72(12):4477–4479, December 2001. URL `http://link.aip.org/link/?RSI/72/4477/1`.