

El Gamal Mixnets and Implementation of a  
Verifier  
SA104x Degree Project in Engineering Physics  
KTH Royal Institute of Technology  
School of Computer Science and Communication  
Supervisor: Douglas Wikström

Carl Svensson carlsven@kth.se & Erik Larsson erikl3@kth.se

April 11, 2013

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>El Gamal Cryptography</b>	<b>2</b>
2.1	Definition . . . . .	2
2.2	Security . . . . .	2
2.3	Properties . . . . .	2
<b>3</b>	<b>Mix Networks</b>	<b>2</b>
3.1	Overview . . . . .	2
3.2	El Gamal Mixnet . . . . .	3
3.3	Operation . . . . .	3
3.4	Verification . . . . .	3
<b>4</b>	<b>Specification/Documentation</b>	<b>3</b>
<b>5</b>	<b>Implementation of the Verifier</b>	<b>3</b>
5.1	General Design Choices . . . . .	3
5.2	Third Party Libraries . . . . .	3
5.2.1	Arithmetic Library . . . . .	3
5.2.2	XML Parser . . . . .	3
5.2.3	Cryptographic Primitives . . . . .	3
5.2.4	Testing . . . . .	3
5.3	Math Library . . . . .	4
5.4	Pseudorandom Generators and Random Oracles . . . . .	4
5.5	Verifier . . . . .	4
5.6	Tests . . . . .	4
5.7	Performance . . . . .	4

<b>6 Conclusion</b>	<b>4</b>
<b>7 References</b>	<b>4</b>

# 1 Introduction

## 2 El Gamal Cryptography

### 2.1 Definition

The El-Gamal cryptosystem is defined over a group  $G_q = \langle g \rangle$  of prime order  $q$ , generated by  $g \in G_q$ . A private key  $x \in \mathbb{Z}_q$  is chosen randomly and is used to compute the public key  $(g, y) \in G_q \times G_q$  where  $y = g^x$ .

Encryption of a plaintext  $m \in G_q$  is done by choosing a random  $s \in \mathbb{Z}_q$  and computing  $(u, v) \in G_q \times G_q$  where  $u = g^s$  and  $v = y^s m$ . Decryption of a ciphertext  $(u, v) \in G_q \times G_q$  is achieved by using the private key  $x$  to compute  $m = u^{-x} v$ .

### 2.2 Security

Let  $b = g^a \in G_q$  where  $a \in \mathbb{Z}_q$ . Then  $a$  is said to be the discrete logarithm of  $b$  in the group  $G_q$ . There is currently no known efficient classical algorithm that given  $(G_q, g, b)$  is able to calculate  $a$  in a reasonable amount of time (polynomial time). The discrete logarithm problem is thus considered to be a hard problem. (Källa)

The security of the El Gamal cryptosystem relies on the difficulty of discrete logarithm in finite cyclic groups  $G_q$ . This means that the El Gamal cryptosystem is secure as long as no one is able to compute the discrete logarithm in  $G_q$  efficiently. (Källa)

### 2.3 Properties

The El Gamal cryptosystem is a homomorphic cryptosystem. This

Generalization

## 3 Mix Networks

### 3.1 Overview

Intuitiv beskrivning (gör bättre)

<http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/universal/Universal.pdf>

One purpose of mix networks, or mixnets, is to provide untraceability to its users. A mixnet may, for example, take as input a list of encrypted messages of different origins. These messages pass through the mixnet and is output decrypted and in a randomized order. This property may be used to enable anonymous voting systems.

A reencryption mixnet consists of a number of servers which sequentially process the messages and reencrypts the list of messages and outputs them in a randomized order. After passing through all servers, the list of ciphertexts is decrypted and the result is a list of the messages in random order. It is impossible to deduce from where each element came.

### **3.2 El Gamal Mixnet**

### **3.3 Operation**

### **3.4 Verification**

## **4 Specification/Documentation**

## **5 Implementation of the Verifier**

### **5.1 General Design Choices**

Programming language?

### **5.2 Third Party Libraries**

#### **5.2.1 Arithmetic Library**

GMP

#### **5.2.2 XML Parser**

RapidXML

#### **5.2.3 Cryptographic Primitives**

OpenSSL

#### **5.2.4 Testing**

Google Test

### **5.3 Math Library**

### **5.4 Pseudorandom Generators and Random Oracles**

### **5.5 Verifier**

### **5.6 Tests**

### **5.7 Performance**

## **6 Conclusion**

## **7 References**