

Family Name: \_\_\_\_\_

First Name: \_\_\_\_\_

Section: \_\_\_\_\_

# Student Seminar: Security Protocols & Applications

Final Exam - Part 1: Ring Signatures

July 16th, 2007

This document consists of 4 pages.

## Instructions

Electronic devices are *NOT allowed*.

Books and lecture notes are *allowed*.

Answers must be written in the boxed spaces provided on these sheets.

Answers can be written either in French or in English.

Questions of any kind by students during the exam will certainly *not* be entertained.

Potential errors in these sheets are part of the exam.

# Ring Signatures

We consider a public key infrastructure which was built to accommodate ring signatures.

1. **A whistle-blowing case.** Alice, Bob, Charly, Dan, and Eve are the top executives in a bank headed by CEO Frank. Alice discovers that the bank is a money laundry for some criminal organization. She wants to disclose this to the press but wants to protect herself. For this, she signs an anonymous letter using ring signatures in a ring consisting of the top executives: Alice, Bob, Charly, Dan, and Eve. Bob and Charly are honest directors who are clueless about these activities, but Dan and Eve are associates of Frank in his criminal activities. Dan, Eve, and Frank decide on all keys to be revoked and the signing keys of all directors to be destroyed. To make it more plausible to the press, Dan's secret key would be anonymously posted on some criminal hacker's web site.

(a) What can the communication representative of the bank tell to the press to claim the innocence of the bank?

(b) Assuming that Alice used the a posteriori anonymity revocation extension of ring signatures, what can she do to a posteriori reduce the ring to Alice, Bob, Charly, and Eve? (Note that she can no longer make any new signature since her key was destroyed.)

2. **Breaking counter-spam protection.** To protect against spamming, it is decided to reject any email that was not signed by the sender. To avoid giving the opportunity to receivers to later transfer binding emails to any third party, a solution is to adopt ring signatures with rings restricted to the sender and the receiver. A receiver Frank wants to cheat with this protection. For this, he declares a public key to the certificate authority for which he owns a proof of ignorance for the secret key. A first idea consists in generating from an arbitrary seed a pseudo-random string that is looking like a public key. The seed would be used as a proof of ignorance of the secret key.

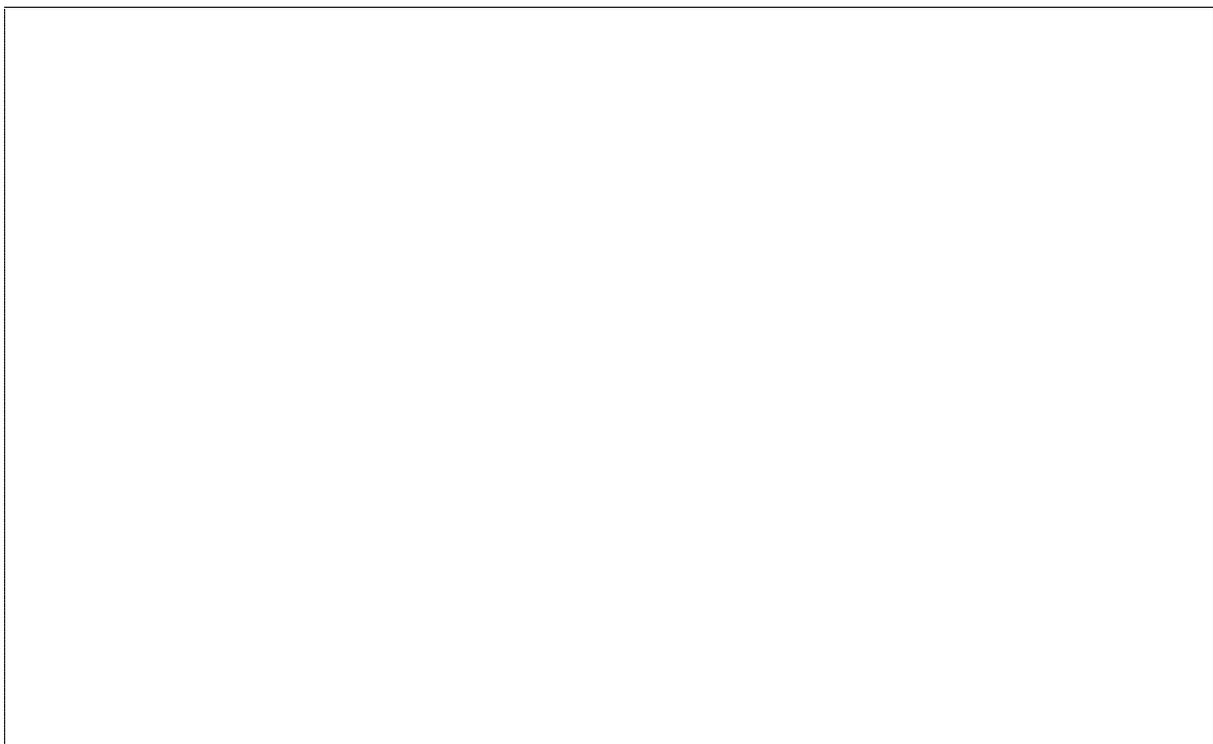
- (a) Explain how Frank can transform an email from Alice to him into digitally signed documents that are binding for Alice.

- (b) Explain how the PKI could protect against this attack.

- (c) By using a tamperproof device with appropriate interface, show that Frank can still register a public key and that the device could be used as a proof of ignorance on the secret key. Sketch an interface for the device.



3. **Escrow ring signature.** We assume that ring signatures are computed by a tamper proof device imposed by the Crook Inc. company. Propose an implementation of it that would make this company see who is the real signer of any ring signature but who would still keep the properties of ring signatures if the company remains silent.



**Any attempt to look at  
the content of these pages  
before the signal  
will be severely punished.**

**Please be patient.**