Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 9

Exercise 9-1 Suppose some message m is encrypted twice using Plain RSA (as in Exercise 8-2) with two different public keys (N, e_1) and (N, e_2). Show that the message m can be recovered without exhaustive search if $\gcd(e_1, e_2) = 1$.

Exercise 9-2 Consider the following key exchange protocol.

- Alice chooses k and r of length n at random and sends $s := k \oplus r$ to Bob.
- Bob generates t of length n at random and sends $u := s \oplus t$ to Alice.
- Alice computes $v := u \oplus r$ and sends it to Bob.
- Alice outputs k and Bob outputs $v \oplus t$.

This protocol allows Alice and Bob to exchange a key k, which they both know at the end.

Is this key exchange protocol secure according to the definition from the lecture? Prove your answer.

Exercise 9-3 A bank uses El Gamal encryption to send transactions over the internet from all branches to the central office. Assume for simplicity that a transaction consists just of the amount x of money to be transferred (and ignore account numbers and the like). The amount x is encoded by the group element g^x, where g is the generator of the group used for encryption.

Suppose you can intercept and manipulate messages. Show how to append a zero to the figure of the amount being transferred in each transaction.

Hint: You do not need to decrypt any messages.