# Exercises 2WC12 week 4

## Exercise 1

For this exercise you may use a computer algebra system or my MCR-software (`http://www.win.tue.nl/~bdeweger/MCR`), but your answer should explain all steps you did, so that a reader who does not have access to this software will be convinced.

a) Alice sends a message $m$ to Bob, Charlie and David, encrypting it with their public RSA keys with moduli 50621, 76693 and 70747, and all three with $e = 3$. The ciphertexts are respectively 884, 10535 and 48241. Recover the plaintext without factoring the moduli.

b) Factor $n = 1441499$ by using that a valid RSA keypair has $e = 17$ and $d = 507905$.

## Exercise 2

a) Let $p$ be prime, and let $a$ ($\not\equiv 0 \pmod p$) be a square $\pmod p$. Prove that $a^{(p-1)/2} \equiv 1 \pmod p$. Also prove that $a$ has exactly two square roots.

b) Let $p$ be prime with $p \equiv 3 \pmod 4$, and let $a$ be a square $\pmod p$. Prove that $\pm a^{(p+1)/4} \pmod p$ are the two square roots of $a$ modulo $p$.

c) Let $p, q$ be primes, and let $n = pq$. Let $a$ (coprime to $n$) be a square $\pmod n$. Prove that there are exactly four square roots.
Hint: look separately modulo $p$ and modulo $q$, and use the Chinese Remainder Theorem.

d) Suppose you know that $n$ is a product of two primes but you don't know the prime factors. Further suppose that you have an efficient method of finding all four square roots of any square. Then show that you can factor $n$.

## Exercise 3

The Rabin cryptosystem works as follows:

– let $p, q$ be primes, and $n = pq$
– the private key is $(p, q)$
– the public key is $(n, B)$, where $B$ is a random integer between 0 and $n$
– encryption of $m$ is $c = m(m + B) \pmod n$
– decryption is solving the encryption equation for $m$ using square roots modulo $n$

We take as private key $(p, q) = (7, 11)$, and as public key $(n, B) = (77, 43)$.

a) Compute the encryption $c$ of the message $m = 23$.

b) Compute all four possible decryptions of $c$.
Hint: use Exercise 2.

**Remark:** Note that, according to exercise 2, breaking Rabin is equivalent to factoring.