

# Exercise 10

## TMA4160 Cryptography, autumn 2007

These exercises are from Trappe and Washington's book "Introduction to Cryptography with Coding Theory", 2nd edition.

**Task 1.** Suppose we use the ElGamal signature scheme with  $p = 65539$ ,  $\alpha = 2$ ,  $\beta = 33384$ . We send two signed messages  $(x, (\gamma, \delta))$ :

$$(809, (18357, 1042))(= \text{hi}) \quad \text{and} \quad (22505, (18357, 26272))(= \text{bye}).$$

a) Show that the same value of  $k$  was used for each signature.

b) Use this fact to find this value of  $k$  and to find the value of  $a$  such that  $\beta = \alpha^a \pmod{p}$ .

**Task 2.** Alice and Bob have the following RSA parameters:

$$\begin{aligned}n_A &= 171024704183616109700818066925197841516671277, \\b_A &= 1571, \\n_B &= 839073542734369359260871355939062622747633109, \\b_B &= 87697.\end{aligned}$$

Bob knows that

$$\begin{aligned}p_B &= 98763457697834568934613, \\q_B &= 8495789457893457345793,\end{aligned}$$

(where  $n_B = p_B q_B$ ). Alice signs a document and sends the document and signature  $(x, s)$  (where  $s \equiv x^{a_A} \pmod{n_A}$ ) to Bob. To keep the contents of the document secret, she encrypts using Bob's public key. Bob receives the encrypted signature pair  $(x_1, s_1) \equiv (x^{b_B}, s^{b_B}) \pmod{n_B}$ , where

$$\begin{aligned}x_1 &= 418726553997094258577980055061305150940547956, \\s_1 &= 749142649641548101520133634736865752883277237.\end{aligned}$$

Find the message  $x$  and verify that it came from Alice.

**Task 3.** In task 2, suppose that Bob had primes

$$\begin{aligned}p_B &= 7865712896579, \\q_B &= 8495789457893457345793.\end{aligned}$$

Assuming the same encryption exponents, explain why Bob is unable to verify Alice's signature when she sends him the pair  $(x_2, s_2)$ , where

$$\begin{aligned}x_2 &= 14823765232498712344512418717130930, \\s_2 &= 43176121628465441340112418672065063.\end{aligned}$$

What modifications need to be made for the procedure to work?