Exam — Security

January 19, 2016. 8:30–11:30

You can score a maximum of 100 points. Each question indicates how many points it is worth. You are NOT allowed to use books or notes, or a (smart) phone. You may answer in Dutch or in English. Read each exercise carefully (RTFE). Please write clearly, and don't forget to put your name and student number on each page that you hand in. Keep the scrap paper for yourself. You can keep this exam too, but don't forget to return the calculator!

Tip: describe the formula or method of calculation explicitly before you start computing; it will give you some points, if correct, even if you don't manage to finish the computation.

1. (**18 points**) Consider the following scenario, where Alice sends a (plaintext) message m to Bob, followed by a message-authentication-code (MAC) on this message m. The goal is to ensure integrity of the message transfer. Different forms of MAC will be considered below.

$$A \longrightarrow B : m, \text{MAC(m)}.$$

Briefly explain for the different MAC options **(a)** – **(c)** below:

- what Bob has to do to check the integrity of the message m; start your answer as follows: Bob receives a pair m', M and ...
- whether or not the particular MAC guarantees integrity; if not, explain how integrity can be compromised.

(a) (**6 points**) MAC$(m) = h(K \mid m)$, where h is a secure hash function, K is a secret key that only A, B know, and | is used for concatenation;

(b) (**6 points**) MAC$(m) = [m]_{d_A}$, where d_A is the private RSA key of Alice.

(c) (**6 points**) MAC$(m) = K \oplus m$, where $\oplus$ is bitwise XOR, and K is a secret key that only A, B know (of the same length as the message m).

2. (**18 points**) Suppose Alice and Bob have agreed on a shared a key K, when they physically met a long time ago. At this moment Alice wants to check that Bob still possesses this same key K. She sends Bob the following (plaintext) message.

$$A \longrightarrow B : \text{“Hi Bob, prove to me that you still have our secret key”} \qquad (*)$$

We consider the following three different options **(a)** – **(c)** for follow-up messages to this protocol line $(*)$. Assume that h is a cryptographic hash function. The main questions for each of the three cases below are whether Bob's answer is convincing and, whether an attacker can obtain the key K.

(a) (**6 points**) Bob answers $(*)$ directly by:

$$B \longrightarrow A : \text{“here is its hash”}, h(K)$$

Is this convincing and secure? Which property of the hash function h are required?

(b) (**6 points**) The protocol $(*)$ now continues as:

$$\begin{aligned} &A \longrightarrow B : N && \text{(a fresh nonce)} \\ &B \longrightarrow A : h(N \mid K) && \end{aligned}$$

You may now assume that h is a secure hash function. Is this convincing and secure? What advantages, if any, does this protocol offer with respect to the previous one?

(c) (**6 points**) Consider now the follow-up steps to $(*)$ described below, where $\oplus$ is bitwise XOR, like before.

$$\begin{aligned} &A \longrightarrow B : X, && \text{where } X = K \oplus N \text{ and } N \text{ is a fresh nonce, with the length of } K \\ &B \longrightarrow A : Y, && \text{where } Y = X \oplus K \end{aligned}$$

Is this convincing and secure?

3. (**12 points**) For this exercise, assume that x is a natural number.

   (a) (**6 points**) Consider the function $h(x) = 3x+2 \mod 9$ as hash function. Show that it is not second pre-image resistant, starting with input $x = 3$.

   (b) (**6 points**) Consider $h(x) = 5x+3 \mod 11$ and show that it is not collision resistant.

4. (**28 points**) Take $p = 7$ and $q = 23$ as prime numbers for RSA.

   (a) (**4 points**) Compute n and $\varphi(n)$.

   (b) (**4 points**) We could set the public exponent $e = 3$. Why does that not work out?

   (c) (**6 points**) Instead, we set $e = 5$. Find the corresponding private exponent d. Describe your computations.

   (d) (**8 points**) Sign the message $m = 17$ to obtain signature s. Include calculation details.

   (e) (**6 points**) Verify the signature s. Show how you do this.

5. (**24 points**) Consider the ElGamal encryption scheme with generator $g = 2$, modulo $p = 19$, private key $x = 7$ and public key $y = g^x = 2^7 = 14 \mod 19$.

   (a) (**6 points**) Decrypt the cipher text (c_1, c_2), where $c_1 = 13$ and $c_2 = 4$.

   (b) (**6 points**) Let $s = 6$. Now compute the pair $(d_1, d_2) = (g^s \cdot c_1, y^s \cdot c_2) \mod p$.

   (c) (**6 points**) Decrypt the cipher text (d_1, d_2) that you obtained in **(b)**.

   (d) (**6 points**) Now assume s is any random number and that (c_1, c_2) is an arbitrary cipher text. Prove that in general the re-randomised cipher text $(g^s \cdot c_1, y^s \cdot c_2)$ decrypts to the same message as (c_1, c_2).