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**) (protocols, hashing, public key crypto, one-time-pad)
   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.

   Begin Secret Info: .....

Grading for all sub-questions (6 points each):	
aspect:	*points*
Correct integrity check method	*2*
if secure:	
For stating that the scheme is secure	*4*
For giving an (unneeded) incorrect argument	*-2*
if not secure:	
For stating that the scheme is not secure	*2*
For briefly explaining why	*2*

   End Secret Info .....

   (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 $\mid$ is used for concatenation;

   Begin Secret Info: .....
   Upon receiving m', MAC Bob checks if $h(K \mid m') = MAC = h(K \mid m)$, if so, then m' is the original message m that A sent.

This is secure, since an attacker does not have K, and so cannot produce a valid MAC $h(K \mid m')$ for an altered message m'.

End Secret Info .....

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

Begin Secret Info: .....
Upon receiving m', MAC Bob uses Alice's public key e_A to turn $MAC = [m]_{d_A}$ into m, and checks if $m = m'$.
This is secure, because an attacker does not have Alice's private key d_A, and so cannot produce such a MAC $[m']_{d_A}$ for a modified message m'.
***Erratum:** Specifically for RSA, however, this is not secure. This is due to the malleability of RSA ciphertexts, allowing an attacker to randomize both m and $[m]_{d_A}$ to obtain m' and $[m']_{d_A}$. Similarly, one could simply take a random number r, use that as value for the MAC, and derive $m' = [r]_{e_A}$.*
As we had also overlooked this initially, accept both interpretations.
End Secret Info .....

(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).

Begin Secret Info: .....
Upon receiving m', MAC, Bob computes $m = K \oplus MAC$, and checks if $m = m'$.
This is not secure, since an attacker can obtain $K = m \oplus$ MAC$(m) = m \oplus (K \oplus m)$. Then he can send his own modified message $m', K \oplus m'$, which passes the test by Bob.

End Secret Info .....

2. (**18 points**) hash functions, protocols, one-time-pads
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?

Begin Secret Info: .....
Yes, this is convincing if the hash function is collision-resistant and/or second pre-image resistant and secure if the hash function is one-way.
Explanation:

- *If Bob chooses a different key K' and hashes it instead of K by mistake, then the resulting hash $h(K')$ must not equal $h(K)$. This means that the hash function must be collision-free. Then Alice can be convinced that the hash she has received from Bob is indeed the hash of the key K, not of any arbitrary key K'.*
- *Alice expects the hash of key K; if Bob manages to find another input K' such that $h(K) = h(K')$, then he could still convince Alice (maliciously). So the hash function should also be second-preimage resistant to convince Alice.*

Grading (total 6):	
aspect:	*points*
Collision resistance	*3*
One wayness	*3*

End Secret Info .....

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

$$A \longrightarrow B : N \qquad \text{(a fresh nonce)}$$
$$B \longrightarrow A : h(N \mid K)$$

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?

Begin Secret Info: .....
This protocol is equally convincing. In the case of the first protocol, attacker can reply with the intercepted message $h(K)$, and make Alice think that Bob still has K, whereas he may have lost K. The current protocol has advantages over the first protocol because if Alice poses the same question again in the future with a different nonce, an attacker cannot replay the hash of the key with the old nonce. But if it is a one time query from Alice, then adding nonce does not make much difference. From that perspective the advantage gained by this protocol is small.

Grading (total 6):	
aspect:	*points*
replay possibility	*6*

End Secret Info .....

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

$A \longrightarrow B : X$, where $X = K \oplus N$ and N is a fresh nonce, with the length of K
$B \longrightarrow A : Y$, where $Y = X \oplus K$

Is this convincing and secure?

Begin Secret Info: .....
This is insecure (and thus not convincing after the first run): the attacker can obtain $X \oplus Y = K \oplus N \oplus K \oplus N \oplus K = K$.

Grading (total 6):	
aspect:	*points*
For pointing out that it is insecure	*2*
Correct method to obtain the key K	*4*

End Secret Info .....

3. (**12 points**) (hash properties, modular arithmetic)
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 $x = 3$.

Begin Secret Info: .....
We have $h(1) = 5, h(2) = 8, h(3) = 2, h(4) = 5, h(5) = 8, h(6) = 2$. *Hence we found another input, namely* 6 *with* $h(6) = 2 = h(3)$.

Grading (total 6):	
aspect:	*points*
$h(3) = 2$	*2*
correct form: we need to find x *with* $h(x) = h(3)$	*2*
correct calculations	*2*

End Secret Info .....

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

Begin Secret Info: .....
$h(1) = 8, h(2) = 2, h(3) = 7, h(4) = 1, h(5) = 6, h(6) = 0, h(7) = 5, h(8) = 10, h(9) = 4, h(10) = 9, h(11) = 3, h(12) = 8$. *Hence* $h(1) = h(12)$.

Grading (total 6):	
aspect:	*points*
correct form: we need to find x, y *with* $h(x) = h(y)$	*2*
correct calculations	*4*

End Secret Info .....

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

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

Begin Secret Info: .....

$n = p \cdot q = 7 \cdot 23 = 161$, $\varphi(n) = (p-1) \cdot (q-1) = 6 \cdot 22 = 132$.

Grading (total 5):	
aspect:	*points*
Correct formula for n and $\varphi(n)$	*2*
Correct computation	*2*

End Secret Info .....

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

Begin Secret Info: .....

We need e and $\varphi(n)$ to be co-prime, i.e. $gcd(e, \varphi(n)) = 1$.

Grading (total 5):	
aspect:	*points*
Correct explanation	*4*

End Secret Info .....

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

Begin Secret Info: .....

We need to invert $e \mod \varphi(n)$, i.e. *find* d *such that* $d \cdot 5 \equiv 1 \mod 132$.
$132 - 26 \cdot 5 = 2$
$5 - 2 \cdot 2 = 1$
So $1 = 5 - 2 \cdot (132 - 26 \cdot 5) = 53 \cdot 5 - 2 \cdot 132$, *so* $d = 53$.

Grading (total 6):	
aspect:	*points*
Correct computation	*3*
correct value of d	*3*

End Secret Info .....

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

Begin Secret Info: .....

$s = m^d = 17^{53} \equiv 145 \mod 161$

Explicitly, via square and multiply:

$$
\begin{aligned}
17^{53} &= 17 \cdot (17^2)^{26} \\
&= 17 \cdot 128^{26} && \textit{since } 17^2 = 289 = 128 \\
&= 17 \cdot (128^2)^{13} \\
&= 17 \cdot (123)^{13} && \textit{since } 128^2 = 16384 = 16384 - 101 \cdot 161 = 123 \\
&= 17 \cdot 123 \cdot (123^2)^6 \\
&= 2091 \cdot (-5)^6 && \textit{since } 123^2 = 15129 = 15129 - 94 \cdot 161 = -5 \\
&= 159 \cdot ((-5)^2)^3 \\
&= 159 \cdot 25^3 \\
&= 159 \cdot 25 \cdot 25^2 \\
&= 111 \cdot 625 \\
&= 111 \cdot 142 \\
&= 15762 \\
&= 145.
\end{aligned}
$$

Grading (total 8):	
aspect:	*points*
Correct formula for signature	*2*
application of square and multiply method	*2*
correct computation	*4*

End Secret Info .....

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

Begin Secret Info: .....

$m = s^e = 145^5 \equiv 17 \mod 161$

Explicitly:

$$
\begin{aligned}
145^5 &= 145 \cdot (145^2)^2 \\
&= 145 \cdot 95^2 && \textit{since } 145^2 = 21025 = 21025 - 130 \cdot 161 = 95 \\
&= 145 \cdot 9 && \textit{since } 95^2 = 9025 = 9025 - 56 \cdot 161 = 9 \\
&= 1305 \\
&= 1306 - 8 \cdot 161 \\
&= 17
\end{aligned}
$$

Grading (total 6):	
aspect:	*points*
Correct formula for signature verification	*2*
application of square and multiply method	*2*
correct verification	*2*

End Secret Info .....

5. (**24 points**) ElGamal public key crypto, modular calculation, insight into the cipher
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 $c_2 = 4$.

   Begin Secret Info: .....

   ${c_1}^{-x} \equiv {c_1}^{p-1-x} = 13^{19-1-7} = 13^{11} \equiv 2 \mod 19.$
   Alternative: egcd to compute $c_1^{-1} \equiv 3 \mod 19$*, then* $c_1^{-x} = (c_1^{-1})^x = 3^7 \equiv 2 \mod 19$.
   $m = c_2 \cdot {c_1}^{-x} = 4 \cdot 2 = 8.$
   Another, complicated version that students will probably follow:

$$\begin{aligned} c_1^x &= 13^7 \\ &= 13 \cdot (13^2)^3 \\ &= 13 \cdot 169^3 \\ &= 13 \cdot 17^3 \\ &= 13 \cdot 17 \cdot 17^2 \\ &= 221 \cdot 289 \\ &= 12 \cdot 4 \\ &= 48 \\ &= 10. \end{aligned}$$

   Next, $\frac{1}{10} \mod 19 = 2$*, since* $2 \cdot 10 = 20 = 1$*. Hence:*

$$\frac{c_2}{c_1^x} = 4 \cdot 2 = 8.$$

Grading (total 6):	
aspect:	*points*
Correct formula	*2*
Correct computation of ${c_1}^{-x}$	*2*
(Correct computation of c_1^x*, if this route is taken*	*1)*
Correct decryption	*2*

   End Secret Info .....

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

   Begin Secret Info: .....

   $(d_1, d_2) = (g^s \cdot c_1, y^s \cdot c_2) = (2^6 \cdot 13, 14^6 \cdot 4) \equiv (15, 9) \mod 19$

More explicitly $2^6 = 64 = 7$ *and:*

$$\begin{aligned} 14^6 &= (14^2)^3 \\ &= 196^3 \\ &= 6^3 \\ &= 6 \cdot 36 \\ &= 6 \cdot 17 \\ &= 102 \\ &= 7. \end{aligned}$$

Thus: $(d_1, d_2) = (7 \cdot 13, 7 \cdot 4) = (91, 28) = (15, 9)$

Grading (total 6):	
aspect:	*points*
correct $g^s = 7$	*2*
correct $y^s = 7$	*2*
correct final result	*2*

End Secret Info .....

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

Begin Secret Info: .....

${d_1}^{-x} \equiv {d_1}^{p-1-x} = 15^{19-1-7} = 15^{11} \equiv 3 \mod 19$
$m = d_2 \cdot {d_1}^{-x} = 9 \cdot 3 \equiv 8 \mod 19$
Explicit route:

$$\begin{aligned} d_1^x &= 15^7 \\ &= 15 \cdot (15^2)^3 \\ &= 15 \cdot 225^3 \\ &= 15 \cdot 16^3 \\ &= 15 \cdot 16 \cdot 16^2 \\ &= 240 \cdot 256 \\ &= 12 \cdot 9 \\ &= 72 \\ &= 13. \end{aligned}$$

We have $\frac{1}{13} = 3 \mod 19$ *since* $3 \cdot 13 = 39 = 1$. *Hence:*

$$\frac{d_2}{d_1^x} = 9 \cdot 3 = 27 = 8.$$

Note that solutions that use a (valid) proof obtained in ***(d)*** *are also accepted.*

Grading (total 6):	
aspect:	*points*
Correct formula	*2*
Correct computation of $d_1{}^{-x}$	*2*
(Correct computation of d_1^x*, if this route is taken*	*1)*
Correct decryption	*2*

End Secret Info .....

(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).

Begin Secret Info: .....

$(g^s \cdot c_1, y^s \cdot c_2)$ *decrypts to:*

$$\frac{y^s \cdot c_2}{(g^s \cdot c_1)^x} = \frac{(g^x)^s \cdot c_2}{(g^s)^x \cdot c_1^x} = \frac{g^{xs} \cdot c_2}{g^{xs} \cdot c_1^x} = \frac{c_2}{c_1^x}$$

which is also the decryption of (c_1, c_2)*.*

Grading (total 4):	
aspect:	*points*
apply correct decryption formula	*2*
distribute exponent correctly	*2*
correct cancelling	*2*

End Secret Info .....

Begin Secret Info: .....

Finally we have a ***toetsmatrix****, relating the original goals of the course to the exercises:*

goal	***exercise***
recognise security goals	*1, 2*
hash functions	*1,2,3*
public key crypto	*4,5*
secret key crypto	*1,2*
protocols	*1,2*

End Secret Info .....