Exam Security

22 January 2013, 10:30 – 12:30

You can score a maximum of 100 points. Each question indicates how many points it is worth. You are NOT allowed to use a book/slides/notes etc, and also NOT to use a calculator, (smart) phone or other device. You may answer in Dutch or in English. Please write clearly, and don't forget to put your name and student number on each page.

1. In this exercise the correct answer may involve more than one option; explain your choice(s) in one or two lines.

   (a) **(5 points)** Consider the situation where a bank customer withdraws money from a cash machine. An essential part of the procedure is the customer typing in his/her PIN. From the bank's perspective, which security goal(s) is/are achieved by this PIN entering?

   i. Confidentiality
   ii. Integrity
   iii. Authentication
   iv. Non-repudiation

   Solution: ....

   Authentication, since a PIN is proof of identity (something you know)

   Non-repudiation, since when you complain to a bank about an incorrect withdrawal, whereas the correct PIN has been used, the bank will not refund.

   ....

   (b) **(5 points)** Now consider a situation where the bank customer does an electronic money transfer (via e-banking) at home: after filling in the transaction details on a webpage, the user has to insert his/her own bank card into a special device (like a "random reader" or "e-identifier") provided by the bank, and type the PIN; the amount involved and destination account also has to be entered into the device. The device then shows a number on its display that the customer has to type into the webpage. Again, from the bank's perspective, for which goal(s) is this procedure designed:

   i. Confidentiality
   ii. Integrity
   iii. Authentication
   iv. Non-repudiation

   Solution: ....

   Integrity, since the amount of money is incorporated into the returned number on the display

   Authentication and non-repudiation, via the bankcard and the PIN, as in the previous question.

   ....

   (c) **(5 points)** When submitting a *paper* tax form, a citizen has to *physically* sign the submitted form. Which goal(s) does this traditional "wet" signature have for the tax office?

   i. Confidentiality
   ii. Integrity
   iii. Non-repudiation

   Solution: ....

   Non-repudiation, since the citizen can be held responsible for the contents through the signature

   ....

   (d) **(5 points)** Next, consider the electronic version of the tax form. When submitting it electronically (in the Netherlands), one has to login via DigiD, upload the form, and then press "submit". Argue briefly why the "non-repudiation" goal is *not* properly realised in this manner.

   Solution: ....

   DigiD is for authentication only and does not provide a signature.

More explicitly, if I login with DigiD, upload the form, but do not press "submit", a system administrator can add this press event to the event log later without any interaction from my side: there is no logical connection between the document and signature data that can only be produced by me.

. . . .

2. **(15 points)** Assume that you obtain an RSA public key (n, e) where n is only 512 bits long. This modulus is so short that brute-forcing is possible. Explain what the consecutive steps are that you have to perform to break this public key by brute-forcing.

Solution: . . . .

(a) *find prime factorisation* $n = p \cdot q$

(b) *compute* $\varphi(n) = (p-1)(q-1)$

(c) *compute private key* $e^{-1} \mod \varphi(n)$ *using the extended Euclidean algorithm.*

. . . .

3. We call an encryption system *commuting* when encrypting a message twice, with different keys, the order of the two encryptions does not matter. Explicitly, with symmetric notation:

$$K_1\{K_2\{m\}\} = K_2\{K_1\{m\}\}$$

Briefly explain your answer to each of the following questions.

(a) **(5 points)** Is Caesar encryption commuting? A key is a number k in this substitution cipher so that encryption with k means that each letter in the plaintext is shifted k positions forwards in the alphabet.

Solution: . . . .

Obviously, first shifting k_1 positions forward and then k_2 positions, is the same as first shifting k_2 positions forward and then k_1. In both cases the result is shifting by $k_1 + k_2$ positions forward.

. . . .

(b) **(5 points)** Is one-time pad encryption commuting?

Solution: . . . .

We reason bit-wise. Let b, k_1, k_2 be bits, and $\oplus$ XOR. Then, by associativity and commutativity of $\oplus$:

$$\begin{array}{rcl} (b \oplus k_1) \oplus k_2 & = & b \oplus (k_1 \oplus k_2) \\ & = & b \oplus (k_2 \oplus k_1) \\ & = & (b \oplus k_2) \oplus k_1. \end{array}$$

. . . .

(c) **(5 points)** Same question for RSA (in pure form, not as some PKCS standard). You may assume that all keys have the same modulus n.

Solution: . . . .

$m^{e_1 \cdot e_2} \mod n = m^{e_2 \cdot e_1} \mod n$.)

For two public keys (e_1, n) and (e_2, n) we have:

$$\begin{array}{rcl} \{\{m\}_{e_2}\}_{e_1} & = & (m^{e_2})^{e_1} \mod n \\ & = & m^{e_1 \cdot e_2} \mod n \\ & = & m^{e_2 \cdot e_1} \mod n \\ & = & (m^{e_1})^{e_2} \mod n \\ & = & \{\{m\}_{e_1}\}_{e_2} \end{array}$$

. . . .

(d) **(5 points)** Explain where precisely the commuting property is used in the following protocol.

$$\begin{array}{lrcl} (1) & A \longrightarrow B & : & K_A\{m\} \\ (2) & B \longrightarrow A & : & K_B\{K_A\{m\}\} \\ (3) & A \longrightarrow B & : & K_B\{m\} \end{array}$$

Here K_X is a secret key which is known only to X.

Solution:
In step (2) A receives the message $K_B\{K_A\{m\}\}$, which is by commutativity the same as $K_A\{K_B\{m\}\}$. A can remove her own decryption from the latter message, which results in the message $K_B\{m\}$ that she subsequently sends to B.

(e) **(2 points)** Which security goal does this protocol realise?

Solution:
Confidential transfer of the message m from A to B, since no-one except A, B can read the message. Integrity is not guaranteed by just encrypting; it requires some form of MAC.

(f) **(3 points)** What makes this protocol special, from the perspective of key management?

Solution:
Symmetric crypto is used, but there is no shared key between A and B.

(g) **(5 points)** Describe an "implementation" of this protocol with padlocks and boxes. The key of X then consists of a personal padlock together with the padlock's key. Encryption $K_X\{m\}$ means putting message m in a box locked with X's padlock.

Solution:
A puts m in the box and locks the box with her own padlock and then sends it to B; B adds his own lock to the lid, and sends the box back. A then removes her own lock, so that the box remains locked with only B's lock. Here the commutativity of the locking plays a role. B can finally remove his own lock and obtain the message m.

4. The following "authenticated key exchange" protocol, where $\mathcal{H}$ is a hash-function, can be used to obtain a fresh session key:

$$\begin{array}{lrcl} 1. & A \longrightarrow B & : & A, N_A \\ 2. & B \longrightarrow A & : & N_B, \mathcal{H}(K_{AB}, N_A) \\ 3. & A \longrightarrow B & : & \mathcal{H}(K_{AB}, N_A + 1, N_B + 2) \end{array}$$

The key K_{AB} is a key shared in advanced only between Alice and Bob. At the end of the protocol the new shared session key is given by $\mathcal{H}(K_{AB}, N_A, N_B)$.

(a) **(4 points)** Does this protocol involve one-way or two-way authentication; explain briefly who knows what after which protocol step.

Solution:
Mutual authentication: A knows she is talking to B after line 2, since only B can produce this message with key K_{AB}, and B knows he is talking to A after message 3, also involving the shared key K_{AB}, but now used in a different manner.

(b) **(6 points)** Explain briefly which of the following three properties of hash function $\mathcal{H}$ are important when the protocol is used in this way.

(C) collision resistance

(P) preimage resistance

(P2) second preimage resistance.

Solution: ....

(C) not important, attacker has no control over the input, (P) important, if the right preimage leaks the key K_{AB} is no longer safe, (P2) same as with (C) not important, no control over (all) inputs.

....

After using the above protocol Alice and Bob exchange messages m_1 and m_2 in the following way:

$$\begin{array}{rl} 4.\ A \longrightarrow B & : \ \mathcal{H}(K_{AB}, N_A, N_B) \oplus m_1 \\ 5.\ B \longrightarrow A & : \ \mathcal{H}(K_{AB}, N_A, N_B) \oplus m_2 \end{array}$$

where $\oplus$ is bitwise exclusive disjunction (XOR).

(c) **(5 points)** What is wrong with this approach? How can the problem be avoided?

Solution: ....

We now use the key as a one-time pad, hence it should only be used once, and not twice as is done here. You can fix this by: (1) Using a better/different encryption scheme, (2) By deriving new sessions keys for example (in general) by setting $\mathcal{H}(K_{AB}, N_A + 2 + i, N_B + 2 + i)$. As the given protocol only consists of 2 uses of a key, any solution where in (4) and (5) a different key (but not $\mathcal{H}(K_{AB}, N_A + 1, N_B + 2)$!) is used is also good for full points. Note: using K_{AB} directly as a key is not *good, give 0 points for this.*

....

5. The so-called Schnorr signature scheme uses a similar setting as ElGamal. It uses a group $\mathbb{Z}_p^*$ where p is a prime number, with a fixed element $g \in \mathbb{Z}_p^*$. The order of g (i.e. the least positive exponent a such that $g^a \equiv 1 \pmod{p}$) has to be a prime q. In this system $x \pmod{q}$ is the private key while $y = g^x \pmod{p}$ is the public key. Signing a message m involves the following steps.

   i. Generate a random temporary key $0 < k < q$.
   ii. Calculate $r = g^k \pmod{p}$.
   iii. Calculate $e = \mathcal{H}(m \parallel r)$
   iv. Calculate $s = k + x \cdot e \pmod{q}$

   The resulting signature is then the pair (r, s). To verify a signature (r, s) on the message m do:

   i. Compute $e = \mathcal{H}(m \parallel r)$.
   ii. The signature is valid if $r \cdot y^e \equiv g^s \pmod{p}$.

   We will now work on a small example problem. Take $p = 43$, so we work in $\mathbb{Z}_{43}^*$ and take $g = 4$. Furthermore, we use the (completely insecure) hash function $\mathcal{H}(m \parallel r) = m \cdot r \pmod{p}$.

   (a) **(5 points)** What is the order of g in $\mathbb{Z}_{43}^*$? Verify that this order is prime.

   Solution: ....

   For the order we find $g^0 = 1, g^1 = 4, g^2 = 16, g^3 = 21, g^4 = 41, g^5 = 35, g^6 = 11, g^7 = 1 \pmod{43}$, so the order is 7, which is prime. Also note that in the next step only the calculation of s depends on this, nothing else in this exercise does.

   ....

   (b) **(5 points)** Compute the signature on $m = 5$ using $k = 3$ and private key $x = 4$.

   Solution: ....

   $r \equiv g^k \equiv 4^3 \equiv 21$, $e = \mathcal{H}(m \parallel r) = m \cdot r = 5 \cdot 21 = 105 \equiv 19 \pmod{43}$, $s = 3 + 4 \cdot 19 = 79 \equiv 2 \pmod{7}$, so the signature is $(21, 2)$

   ....

   We will now verify a signature on the message $m = 42$. The signature is given by $(r, s) = (41, 2)$ the public key of the signer is known to be $y = 11$.

   Solution: ....

   The private key is $x = 6$ in this case, $k = 4$

   ....

(c) **(3 points)** First compute e; provide intermediate calculation results.
(This can be done by hand; it may look difficult, but it is not; if you do not finish the computation, continue with value $e = 2$.)

Solution: ....

$e = \mathcal{H}(m \parallel r) = 42 \cdot 41 = 1722 = 40 \cdot 43 + 2 \equiv 2 \pmod{43}$ *(Observation for making the computation even easier:* $42 \cdot 41 \equiv (-1)(-2) \equiv 2 \pmod{43}$.*)*

....

(d) **(7 points)** Then compute both $r \cdot y^e$ and g^s. Is the signature valid?

Solution: ....

$r \cdot y^e \equiv 41 \cdot 11^2 = 41 \cdot 121 \equiv 41 \cdot 35 = 1435 = 33 \cdot 43 + 16 \equiv 16$

$g^s \equiv g^2 \equiv 4^2 \equiv 16$. *So the signature is correct.*

....