Re-Exam Security

7 May 2015, 8:30–10:30

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. You can keep this exam yourself.

1. (**22 points**) Consider the next two protocols between Alice and Bob. They each have their own RSA modulus, public, and private exponents (n_A, e_A, d_A) and (n_B, e_B, d_B); h is a (secure) hash function.

$$(1)\quad \begin{cases} A \longrightarrow B : \text{contract} \\ B \longrightarrow A : \text{ok} \\ A \longrightarrow B : h(\text{constract}) \\ B \longrightarrow A : [h(\text{constract})]_{d_B} \end{cases} \qquad (2)\quad \begin{cases} A \longrightarrow B : \{N_A\}_{e_B} \\ B \longrightarrow A : N_A, \{N_B\}_{e_A} \\ A \longrightarrow B : N_B \end{cases}$$

   The hash values $h(x)$ and nonces N_A and N_B all have a length of 128 bits. Alice and Bob use the same keys for both protocols.

   (a) (**4 points**) What is the goal of protocol (1)? Give a brief and concise description.

   (b) (**6 points**) What does Bob need to check at which stage in protocol (1)? What should Alice check?

   (c) (**4 points**) What is the goal of protocol (2)?

   (d) (**8 points**) Check if there is a protocol run that is part of (1), (2) or both, in which an evil party Eve (E) makes Bob sign a bad contract (bad for Bob). If so, use protocol notation to describe this protocol run, as above, and briefly explain why your answer works.

2. (**20 points**) Alice and Bob have a shared symmetric key K_{AB} which they can use for exchanging encrypted messages. They are worried that their messages may become eventually known to someone who intercepts all ciphertexts, for instance because the key K_{AB} is stolen or lost at some stage. They are interested in obtaining higher levels of confidentiality.

   They agree to do the following, using a hash function h. For their first message they use K_{AB} as encryption key, for the second message they use $h(K_{AB})$ instead, for the third $h^2(K_{AB}) = h(h(K_{AB}))$, ..., for the $(n+1)$-th message they use $h^n(K_{AB})$ as encryption key.

   Briefly explain your answers to the following questions.

   (a) (**10 points**) What do Alice and Bob have to keep and what to throw away at stage n? Which property of the hash function h is essential?

   (b) (**10 points**) With this scheme Alice and Bob wish to achieve both *forward* and *backward* secrecy. Forward secrecy means that if ever key n leaks, messages $n+1$ and higher are still protected. Backward secrecy means the opposite, so if ever key n leaks, messages $n-1$ and lower are still protected. Does this scheme provide Alice and Bob with, forward secrecy, backward secrecy, or both?

..... **The exam continues on the next page!** .....

3. (**32 points**) This exercise considers digital (money) cheques. Assume that with each bank account a public key pair is associated, where only the bank account holder knows the private key. The bank has its own private key.

   If person X requests a cheque from his/her bank, the bank returns a signed message of the following form.

$$C_0 = [(X\text{'s account number}, \text{amount})]_{\text{bank's private key}}$$

   In doing so the bank takes 'amount' form X's bank account. Person X can now pass the cheque to person Y by giving him/her

$$C_1 = [(Y\text{'s account number}, C_0)]_{X\text{'s private key}}$$

   If Y wants, now he/she can pass the cheque to person Z by giving

$$C_2 = [(Z\text{'s account number}, C_1)]_{Y\text{'s private key}}$$

   Et cetera.

   (a) (**8 points**) Suppose you receive a cheque at stage C_n. What do you have to verify in order to gain certainty about the integrity of this payment to you? Be very precise!

   (b) (**4 points**) What privacy-sensitive information do you learn when you receive a cheque at stage n?

   (c) (**6 points**) What does the bank verify when eventually cheque C_n is cashed? What happens when C_n is found correct by the bank?

   (d) (**6 points**) Consider the problem of double (or multiple) spending. Explain briefly:

      i. what the problem is

      ii. who can detect it at what stage in the chain (assuming that there is no communication between the parties involved)?

      iii. whether the perpetrator (*dader*) can be identified, and if so, by whom?

   (e) (**8 points**) Modify the scheme so that every cheque C_k also includes a transaction identifier I_k (*e.g.* a counter) which is fresh in this chain. In order to prevent double spending, what message should I now send to the bank when I receive cheque C_{n+1}, and what answer do I expect? Think/explain carefully!

4. (**26 points**) Consider the RSA crypto-system, with primes $p = 5, q = 11$ and public exponent $e = 29$.

   (a) (**12 points**) What is the associated private key? Write down all the intermediate steps, including the steps of the extended-greatest-common-divisor calculation.

   (b) (**14 points**) Encrypt the message "papa" in ECB mode, with encoding 'a' = 2, 'b' = 3, etc. Explain how you proceed.