Exam Security

12 April 2010, 8:30 – 10:30

You can score a maximum of 100 points. Each question indicates how many points it is worth. You may answer in Dutch or in English. Please write clearly, and don't forget to put your name on each page.

1. In security engineering, a nonce is an abbreviation of *number used once*. It is often a random or pseudo-random number which is used in a security protocol.

   (a) **(5 points)** Why, in general, should a nonce only be used once?

   (b) **(5 points)** What does it mean when one talks about a *pseudo*-random number generator?

   (c) **(5 points)** Which implicit assumption is made when timestamps are used as nonces?

2. The Mifare Classic is an RFID chip with a globally unique unchangeable identification number called UID, and some memory which can be read and written. To perform these memory operations one has to know the corresponding keys in order to gain access to the chip. The UID is used to recognise cards, and to block them in case of fraud.

   In 2008, research by the Digital Security group has revealed a security vulnerability in Mifare Classic RFID chips that affects many applications using these chips. One of these applications is the OV-chipkaart. Exploiting this vulnerability one can extract the keys from the chip, and hence read all the data stored inside and change it (except for the UID). Typically this turns an OV-chipkaart into an open wallet, since all data can be read and written. Especially, you can increase the balance on your own card and thus make free trips.

   Assume you are working for TLS, the issuer of the OV-chipkaart, and you must prevent that cardholders make free trips; you can use cryptographic means only, and not for instance shadow bookkeeping of cards in the back-office.

   Briefly discuss (in one or two lines) if the proposals below prevent free trips; if not, indicate a fraud scenario.

   (a) **(3 points)** Encrypt the balance (saldo) on the card (with a secret key only known to TLS).

   (b) **(3 points)** Encrypt all data on the card (with a secret key only known to TLS).

   (c) **(3 points)** Sign the UID of the card (with a private key only known to TLS).

   (d) **(3 points)** Sign the balance on the card (with a private key only known to TLS).

   (e) **(3 points)** Sign all data, including the UID, on the card (with a private key only known to TLS).

   (f) **(3 points)** Use a combination of signing and encryption.

   (g) **(3 points)** Use a random UID instead of a fixed UID.

3. Let H be a secure hash function that meets the conditions *efficiency* (E), *onewayness* (O) and *collision resistance* (C). Let x_1, x_2, x_3, ... below denote bits and let $x_1 \dots x_n$ denote the concatenation of bits $x_1, \dots, x_n$. The operator $||$ denotes bit-string concatenation. For instance $(01)||(110) = 01110$. The operator $\oplus$ denotes XOR. Let p be a large prime. Consider $\mathbb{Z}_p^*$, the multiplicative group of integers modulo p with generator g.

   Determine for the following functions h which of the properties (O) and (C) hold. Explain your answer briefly.

   (a) **(5 points)** $h(x_1 \cdots x_{2n}) = (x_1 \oplus x_{n+1})|| \cdots ||(x_n \oplus x_{2n})$;

(b) **(5 points)** $h(x_1 \cdots x_{2n}) = H(x_1 \cdots x_n) \oplus H(x_{n+1} \cdots x_{2n})$;

(c) **(5 points)** $h(x) = g^x \mod p$;

(d) **(5 points)** $h(x) = g^{H(x)} \mod p$.

4. Let C_X^Y be (ad hoc) notation for a certificate of X, signed by Y. Assume agents P, Q, R, S and certificates C_Q^P, C_R^P, C_S^R. Assume further that everybody knows his own key pair and also P's public key.

   Explain in a few lines which certificates are needed by both S and Q in order to securely perform the following tasks.

   (a) **(7 points)** S sends a confidential message to Q.

   (b) **(7 points)** S sends a signed message to Q.

5. Consider $\mathbb{Z}_{17}^*$, the multiplicative group of integers modulo 17 and a generator $g = 3$ in this group.

   (a) **(5 points)** How many elements does the group $\mathbb{Z}_{17}^*$ have? List them.

   (b) **(5 points)** For which number n ($n \neq 0$) do we have $3^n = 1 \mod 17$?

   (c) **(10 points)** Compute the ElGamal encryption of a message $m = 4$ using the public key $g^x = 5$ and randomness $r = 3$. Thus: compute the ciphertext $(c_1, c_2) = \{4\}_5$.
   (The private key x is not given, since it is not necessary for encryption.)

   (d) **(10 points)** It is well-known that the security of ElGamal is lost when the same randomness r is used twice. Imagine that Alice is silly enough to ignore this and sends the following ciphertexts: $(c_1, c_2) = (8, 10)$ and $(c_1', c_2') = (8, 13)$. Exploit this mistake to recover the second plaintext message m', knowing that the plaintext of the first message is $m = 4$.
   (Hint: in order to do so you might need to use division modulo 17).