2007 - Exercises IX.

1. Alice wants to login to a computer system and needs to communicate her password to the system.
   Alice uses a wireless keyboard but her husband Bob has infected her computer by a key-logger program. Bob also intercepts wireless communication between the keyboard and the computer. However, neither Alice's display nor the connection between Alice's computer and the system can be monitored.

   Propose a simple protocol that allows Alice to securely authenticate to the system.

2. Let CBC-MAC be of the following form:

   $$\text{CBC-MAC}_k = f_k(f_k(\dots f_k(f_k(m_1) \oplus m_2) \dots \oplus m_{n-1}) \oplus m_n),$$

   where $f_k : \{0,1\}^m \to \{0,1\}^m$ is an encryption function with a key k and $m = m_1||m_2||\dots||m_n$ is a message of length nm.

   (a) Show that CBC-MAC is not secure if messages can be of varying lengths. (Show that if messages have variable length then it is possible to mount a chosen message attack, *ie.* given valid MACs for messages $M_1, M_2, \dots, M_N$, an attacker can produce a valid MAC for a new message $M \neq M_i$.)

   (b) Suppose that we append the length of the message, l, as an extra block at the end ($m = m_1||m_2||\dots||m_n||l$), before computing the MAC. Show that it is still possible to mount a chosen message attack.

3. Consider a generic secret sharing scheme.
   A dealer D wants to share a secret s between n parties so that t of them have no information about s, but $t+1$ of them can reconstruct the secret.

   Let v denote the number of possible values of s and let w denote the number of different possible share values that a given party might receive, as s varies. Assume that w is the same for each party.
   What is the relation between v and w? Explain.

4. There are four people in a room and exactly one of them is an adversary. The other three people share a secret using Shamir's $(3,2)$-secret sharing scheme over $\mathbb{Z}_{11}$. The adversary has randomly chosen a pair of numbers for himself. The four pairs are $(x_1, y_1) = (1,4)$, $(x_2, y_2) = (3,7)$, $(x_3, y_3) = (5,1)$ and $(x_4, y_4) = (7,2)$.

   Determine which pair was created by the adversary. Determine also the shared secret. Explain your reasoning.

5. Let p be a large prime and let $n < p$, $t \leq n \in \mathbb{N}$.
   Propose a protocol which enables n parties to colectivelly choose a secret random number $s \in \{0, \dots, p-1\}$. After executing the protocol the parties should share s using Shamir's (n,t)-secret sharing scheme.

6. Suppose that Alice uses the Okamoto identification scheme with $p = 88667$, $q = 1031$, $\alpha_1 = 58902$ and $\alpha_2 = 73611$.

   (a) Alice chooses exponents $a_1 = 846$ and $a_2 = 515$. Compute in detail v.

   (b) Alice chooses exponents $k_1 = 899$ and $k_2 = 16$. Compute in detail γ.

   (c) Bob sends the challenge $r = 489$ to Alice. Compute in detail Alice's response y_1 and y_2.

   (d) Perform Bob's calculations to verify y_1 and y_2.

7. Consider the following protocol, involving a dealer and n recipients, for distributing information.

   Framework of the protocol is the following:

   - Let t be a fixed number, $0 \leq t \leq n$.
   - Each participant can send a private message to any other participant.
   - The dealer begins with information v.
   - After execution of the protocol, each recipient either accepts or rejects.
   - The dealer and/or up to t recipients may cheat.

   Steps of the protocol are as follows:

   (i) The dealer sends v to each recipient.

   (ii) Each recipient sends to each other recipient the value received in the previous step.

   (iii) Each recipient verifies whether more than t of the values received in the previous step are different from the value received in the first step. If more than t values are different, it sends a complaint to each recipient.

   (iv) Each recipient accepts if it receives at most t complaints (including its own). Otherwise the recipient rejects.

   Answer the following questions. Explain your reasoning.

   (a) Suppose that the dealer is honest. For which t every honest recipient accepts?

   (b) Suppose that the dealer cheats. For which t the honest recipients either all accept or all reject?

   (c) Suppose that no recipient complains in the third step. For which t all honest recipients have the same value from the dealer after the protocol has finished?

   (d) Suppose that the recipients later reconstruct the dealer's value by sending their values to a trusted (and honest) party who decides by majority. Suppose further that the dealer is honest. For which t the values which the cheating recipients send to the trusted party cannot influence the outcome of the reconstruction?