IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises IX.

1. Give an example of an orthogonal array OA$(3, 4, 1)$.

2. Suppose we use Shamir's (n, t)-threshold with $n = 4$ and $t = 3$. Suppose $p = 1234567890133$, x_i and $y_i = a(x_i)$ are as follows:

$$(1, 645627947891),$$
$$(2, 1045116192326),$$
$$(3, 154400023692),$$
$$(7, 973441680328).$$

Find the secret S and the polynomial $a(x)$.

3. We have the following access structure for the players $\{P_1, P_2, P_3, P_4, P_5\}$:

$$\{\{P_1, P_3\}, \{P_2, P_4\}, \{P_1, P_2, P_5\}, \{P_3, P_4, P_5\}\} = \{B_1, B_2, B_3, B_4\}$$

and all their supersets.

Consider the following secret sharing scheme for this access structure: The sets B_i and their ordering is known. Let S be the secret. For every $B_i = \{P_{i_1}, \ldots P_{i_k}\}$ choose k random values a_{i_j} such that

$$a_{i_1} + a_{i_2} + \ldots a_{i_k} = S \bmod 29$$

and give every player P_{i_j} his share $a_{i,j}$. The order of shares given to each player is given by the ordering of B_i.

Suppose the players $\{P_1, P_2, P_3, P_4, P_5\}$ were given the following shares:

$$\begin{array}{lll} P_1: & a_{1,1} = 10, & a_{3,1} = 5 \\ P_2: & a_{2,1} = 17, & a_{3,2} = 4 \\ P_3: & a_{1,2} = 30, & a_{4,1} = 25 \\ P_4: & a_{2,2} = 23, & a_{4,2} = 18 \\ P_5: & a_{3,3} = 2, & a_{4,3} = 26 \end{array}$$

   (a) Show how every group B_i constructs the secret.

   (b) Show that the group $\{P_1, P_4, P_5\}$ cannot construct the secret.

4. Consider the following authentication protocol with two parties A and B and a trusted authority T. The protocols provides authentication between A and B and distribution of a secret key generated by T. The protocol works as follows:

$$\begin{array}{ll} A \longrightarrow B: & M, A, B, \{N_a, M, A, B\}_{K_a} \\ B \longrightarrow T: & M, A, B, \{N_a, M, A, B\}_{K_a}, \{N_b, M, A, B\}_{K_b} \\ T \longrightarrow B: & M, \{N_a, K_{ab}\}_{K_a}, \{N_b, K_{ab}\}_{K_b} \\ B \longrightarrow A: & M, \{N_a, K_{ab}\}_{K_a} \end{array}$$

where A, B are the identifiers of the two parties. N_a, N_b are random nonces generated by their first senders. K_a, respectively K_b, is the secret key shared between A, respectively B, and T (distributed before the start of the protocol). K_{ab} is the distributed secret key intended for securing subsequent communication between A and B. $\{M\}_K$ denotes the message M encrypted by secret key K.

Malicious user C can do a man in the middle attack on A by intercepting her messages to B and impersonating B by sending his own messages. Show that C can convince A he is B and that he can make A use key K_{ab} known to C.

More on next page >>>

5. Secret sharing schemes for general access structures can be constructed by using several independent instances of (k, n) threshold scheme.

   (a) Design a secret sharing scheme for five participants $\{A, B, C, D, E\}$ and access structure $\{\{A, B\}, \{B, C, D\}, \{A, D, E\}\}$ with the use of as few instances of a threshold scheme as possible.

   (b) Which subset of participants can we add to the access structure given in (a) to make it implementable by a singe threshold scheme?

6. Authentication codes use a secret key (shared between Alice and Bob) $k \in K$ to choose function a_k and calculate a tag $t = a_k(m) \in T$ for a message $m \in M$. Then Alice sends message-tag pair (m, t) to Bob, who with the use of k can verify that $a_k(m) = t$.
   Such code can thus also be seen as a set of randomly chosen functions $f_k : M \mapsto M \times T$ and their corresponding inverse verification *partial* functions (*ie.* not defined for all $(m, t) \in M \times T$) $g_k : M \times T \mapsto M$, such that $g(f(m)) = m$. Message (m, t) is accepted only if secret partial function $g_k(m, t)$ is defined for (m, t).

   (a) Suppose $M = \{0, 1\}$, $K = \{0, 1\}^2$ and $T = \{0, 1\}$. Does the set of functions f_k given by the following table provide authentication? Explain your reasoning.

$m \rightarrow$	0	1
f_1	$(0, 0)$	$(1, 0)$
f_2	$(0, 0)$	$(1, 1)$
f_3	$(0, 1)$	$(1, 0)$
f_4	$(0, 1)$	$(1, 1)$

   (b) Suppose that the probability distribution on messages is uniform. Can you change the set of functions f_k in such a way that it would provide authentication as well as perfectly secure encryption? Explain your reasoning.

7. Suppose Alice is using the Schnorr identification scheme with $q = 617$, $p = 4937$, $t = 9$ and $\alpha = 1624$.

   (a) Verify that α has order q in $\mathbb{Z}_p^*$.

   (b) Let Alice's secret exponent be $a = 55$. Compute v.

   (c) Suppose that $k = 29$. Compute γ.

   (d) Suppose that Bob sends the challenge $r = 105$. Compute Alice's response y.

   (e) Perform Bob's calculations to verify y.