*IV054 Coding, Cryptography and Cryptographic Protocols*
**2016 - Exercises IX.**

1. Suppose Alice is using the Schnorr identification scheme with $p = 1031$, $q = 103$, $t = 6$, $\alpha = 10$.
   (a) Verify that $\alpha$ has order $q$ modulo $p$.
   (b) Let Alice's secret be $a = 17$. Compute $v$.
   (c) Suppose that $k = 47$. Compute $\gamma$.
   (d) Suppose that Bob sends as his challenge $r = 61$. Compute Alice's response $y$.
   (e) Perform Bob's calculations to verify $y$.

2. Consider the Shamir's $(n, t)$-threshold scheme. Show that, in the secret reconstruction, a dishonest party can exclusively recover the secret, while forcing other honest parties to derive a faked secret.

3. Give an example of an orthogonal array OA$(2, 5, 2)$.

4. Since Bob knows he is about to lose his memory, he has asked three of his friends $A_1, A_2, A_3$ to remember a secret $S$ for him. To prevent them from knowing $S$ on their own, Bob used an $(3, 2)$-threshold scheme and made sure that they do not know each others identities (*ie.* $A_1$ does not know who $A_2, A_3$ is, and so on), and he told them to come find him in a month, so he can recover the secret $S$.

   However, three of Bob's enemies $E_1, E_2, E_3$ have learned of this, and they decided to prevent Bob from recovering $S$. For this purpose, they decided to use the very same $(3, 2)$-threshold scheme to hide some message $S'$.

   In a month, all of them meet. Can Bob faithfully recover the secret $S$, if he has no idea whom to trust?

5. Consider the following function $f$ that computes the message authentication code of a message $m$ comprising blocks $m_1||m_2||\ldots||m_n$ using a secret key $k$ and a block cipher $E$:
$$f_1 = E_k(m_1),$$
$$f_i = E_k(f_{i-1} \oplus m_i) \quad \text{for } i = 2, \ldots, n$$
   Show that $f_n$ is not a secure message authentication code.

6. Let $(G, \cdot)$ be a group and $s \in G$ be a secret key. Propose a perfect $(n, n)$-threshold scheme based on $G$.

7. Consider the Okamoto identification scheme simplified in the following way: we completely omit the numbers $\alpha_2$, $a_2$, $k_2$ and $y_2$. This means our computation will change in the following way:
$$v = \alpha^{-a_1} \mod p,$$
$$\gamma = \alpha^{k_1} \mod p,$$
$$y_1 = k_1 + a_1 r \mod q$$
   and verification will be
$$\gamma \equiv \alpha_1^{y_1} v^r \mod p.$$
   (We can consider this the case of the original protocol where it always holds $a_2 = k_2 = 0$.)

   Show that if Alice now chooses unfortunate $a_1$ and $k_1$ such that
$$v\gamma \equiv 1 \mod p,$$
   then Bob can discover the secret key $a_1$.

8. Consider a group of $2^n - 1$ users, $n \geq 1$, trying to share a secret. These users are organized in a perfect binary tree hierarchy. Design a secret sharing scheme that will allow the recovery of the secret only to the groups which contain users that form a path from the root of the binary tree to one of its leaves (or more precisely the subgraph induced by this group contains such path).