IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises IX.

1. A company owns a secret know-how. There are three owners, one CEO, and five managers in the company. Design a secret sharing scheme such that at least

   - three owners, or
   - two owners and the CEO, or
   - two owners and two managers, or
   - one owner, the CEO and three managers, or
   - one owner and five managers

   can reveal the secret know-how. Justify your answer.

2. Consider the Okamoto's identification scheme with public $p = 8017$, $q = 167$, $\alpha_1 = 255$ and $\alpha_2 = 616$. Show in detail the steps of identification if Alice has chosen $a_1 = 32$, $a_2 = 87$, $k_1 = 10$, $k_2 = 70$ and Bob's challenge is $r = 777$. (Omit the part of the scheme related to TA's signature.)

3. Find an example of an orthogonal array $\mathrm{OA}(2, 4, 2)$.

4. Consider Shamir's $(5, 3)$-threshold scheme with $p = 500009$.

   (a) Find shares of the threshold scheme with

   $$\begin{aligned} &\{x_i = i\}_{i=1}^{5} \\ &a_1 = 3^{\text{<YOUR UČO>}} \mod 101021 \\ &a_2 = 5^{\text{<YOUR UČO>}} \mod 101021 \\ &S = \text{< YOUR UČO >} \end{aligned}$$

   (b) Reconstruct the secret from the following shares: $(1, 155477)$, $(2, 478688)$, $(3, 471642)$.

5. Consider the Schnorr identification scheme with $p = 311$ and $q = 31 \,|\, (p-1)$. Let $\alpha = 169$, which has order q in $\mathbb{Z}_p^*$. Further, let $v = \alpha^{-a} \equiv 47 \mod p$.

   (a) Which of the following is a transcript (γ, r, y) of a correctly performed execution of the Schnorr identification scheme? (There are multiple correct transcripts).

   $$(225, 21, 9), (225, 17, 19), (225, 19, 29), (225, 11, 23)$$

   (b) Use two of valid transcripts from (a) to recover the secret key a.

6. Can a secret sharing scheme for five participants A, B, C, D, E and an access structure generated by the authorized sets $\{A, B\}$, $\{B, C, D\}$, $\{A, D, E\}$ be implemented using only one instance of a threshold scheme? Prove your answer.

7. Consider the general form of orthogonal arrays:
   A $t - (n, k, \lambda)$ orthogonal array is, for $t \leq k$, a $\lambda n^t \times k$ array, whose entries are from a set of n symbols, such that in any t columns of the array every one of the possible n^t t-tuples of symbols occurs in exactly λ rows.

   (a) Prove that any $t - (n, k, \lambda)$ orthogonal array is also $t' - (n, k, n^{t-t'}\lambda)$ orthogonal array for any $1 \leq t' \leq t$.

   (b) Find all integers $a \geq 2$ such that there exists at least one $(a-1) - (a, a, 1)$ orthogonal array. Prove your answer.