IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises X.

1. Consider the Okamoto Identification Scheme with $p = 7823$, $q = 3911$, $\alpha_1 = 556$ and $\alpha_2 = 1568$. Show in detail the steps of the protocol if $a_1 = 1234$, $a_2 = 524$, $k_1 = 118$ and $k_2 = 2004$ and Bob's challenge is $r = 3015$. For simplification, consider omitting the digital signatures, *ie.* the protocol does not use the trusted authority TA and Alice sends v directly to Bob without the certificate.

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

3. Sender S broadcasts messages to n receivers $R_1, \ldots, R_n$. Privacy is not important, but message authenticity is. Each of the receivers wants to be sure that the messages were indeed sent by S. Users decide to use MAC.

   (a) Suppose all users and S share a secret key k. Sender S adds a MAC to the broadcast message using k and every user verifies it. Explain why this scheme is insecure.

   (b) Suppose sender S has a set $A = \{k_1, \ldots, k_m\}$ of m secret keys. Each receiver has some subset $A_i \subseteq A$ of the keys. Before sending a message, S computes MAC c_i of the message for each key k_i. Then S appends $c_1, \ldots, c_m$ to the message. Receiver R_i accepts the message as authentic if and only if all MACs corresponding to the keys in A_i are valid. Which property should sets $A_1, \ldots, A_n$ satisfy to be resistant to the attack from (a)? Assume that receivers cannot collude.

   (c) Suppose that $n = 6$. What is the minimal number of keys so as the condition from (b) is satisfied? Describe sets $A_1, \ldots, A_6$.

4. There are four people in a room and exactly one of them is an adversary. The other three people share a secret using the 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. Consider the following secret sharing scheme. A secret polynomial $f(x) \in \mathbb{R}[x]$ is given, its absolute term $f(0)$ is the secret. There are six people who know different pieces of information:

   - Alice knows that $\deg f = 3$.
   - Bob knows that $f(1) = 1701$.
   - Charlie knows that $f(-1) = 2299$.
   - Dave knows that f is monic.
   - Emily knows that the linear term of f' is zero.
   - Frank knows that the linear term of f is -300.

   Find the secret and determine all possible groups of people that are together able to determine the secret with certainty.

6. Consider the Okamoto Identification Scheme with public keys p, q, α_1 and α_2. For simplification, consider omitting the digital signatures.

   (a) Given v, show that there are exactly q pairs (a_1, a_2), $0 \leq a_1, a_2 \leq q-1$, such that $v \equiv \alpha_1^{-a_1}\alpha_2^{-a_2} \pmod{p}$ and that for any two such pairs $(a_1, a_2) \neq (a_1', a_2')$ it holds $a_1 \neq a_1'$ and $a_2 \neq a_2'$.

   (b) Suppose that Alice choose the random numbers a_1, a_2, k_1 and k_2 and sends v and γ to Bob according to the protocol. Suppose that as a response to the challenge r Bob receives y_1 and y_2 calculated by Alice according to the protocol. Show that if Alice choose a_1' and a_2' instead of a_1 and a_2 such that $(a_1, a_2) \neq (a_1', a_2')$ and $v \equiv \alpha_1^{-a_1'}\alpha_2^{-a_2'} \pmod{p}$ then there exist k_1' and k_2' such that

$$\gamma \equiv \alpha_1^{k_1'}\alpha_2^{k_2'} \pmod{p},$$

$$y_1 \equiv k_1' + a_1' r \pmod{q} \text{ and } y_2 \equiv k_2' + a_2' r \pmod{q}.$$