IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises IX.

1. *(4 points)* Consider Shamir's $(5, 3)$ threshold scheme with $p = 567997$.
   (a) Find shares of the threshold scheme with
   $$\{x_i = i\}_{i=1}^{5}$$
   $$a_1 = 3^{<\text{YOUR UČO}>} \mod 101021$$
   $$a_2 = 5^{<\text{YOUR UČO}>} \mod 101021$$
   $$S = <\text{YOUR UČO}>$$
   (b) Reconstruct the secret from the following shares: $(1, 438827), (2, 273042), (3, 133864)$.

2. *(4 points)* Consider the Okamoto identification scheme with $p = 311$ and $q = 31|(p-1)$. Let $\alpha_1 = 113$ and $\alpha_2 = 169$, both of which have order 31 in $\mathbb{Z}_p^*$. Further, let $v = \alpha_1^{-a_1}\alpha_2^{-a_2} \equiv 83 \mod 311$.
   (a) Which of the following is a transcript $(\gamma, r, (y_1, y_2))$ of a correctly performed execution of the Okamoto identification scheme? (There are multiple correct transcripts).
   $$(20, 27, (18, 29)),\ (20, 4, (18, 26)),\ (24, 4, (15, 26)),\ (24, 27, (15, 29))$$
   (b) Use two of these valid transcripts to recover the secret keys a_1 and a_2, with the knowledge that instead of choosing new k_1, k_2 at random for each run, Alice uses a pseudorandom update function $(k_1)_{i+1} = 3(k_1)_i + 4 \mod 31, (k_2)_{i+1} = 5(k_2)_i + 3 \mod 31$. Show that the recovered secret keys are correct.

3. *(3 points)* An army controls a powerful missile. They want to distribute a key that can launch it between the Field marshal, ten Generals, fifty Colonels, and hundred Majors.
   They do not want to launch it unless the Field marshal decides to do so, or three Generals decide to do so, or two Generals and five Colonels decide to do so, or one General seven Colonels and fifteen Majors are in favour of doing so. Notice that without a single General any number of Colonels or Majors cannot launch the missile. Can you use a single instance of a threshold secret sharing scheme to fulfill this task? If yes, describe how. Otherwise, prove that it is not possible.

4. *(6 points)*
   (a) Decide whether the following array is an orthogonal $\text{OA}(3, 4, 1)$ array:

0	0	0	0
1	1	1	1
2	2	2	2
0	1	0	2
1	2	2	0
2	0	1	1
0	2	2	1
1	0	1	2
2	1	0	0

   (b) Determine whether there exists the following orthogonal array. Prove your answer.
      i. $\text{OA}(2, 7, 2)$;
      ii. $\text{OA}(2, 8, 2)$.

More on next page >>>

5. *(4 points)* Alice and Bob are using the basic Fiat-Shamir identification scheme. In order to decrease Eve's cheating probability they enhanced the protocol by letting the challenge b be chosen from $\{0, 1, 2, 3\}$ instead of just $\{0, 1\}$. The rest of the protocol is identical to the original version. The idea being that Eve now has to guess two bits instead of just one, halving her probability of cheating.

   (a) Show that this modified protocol still allows Bob to identify Alice.

   (b) Find possible commitments and responses of a cheating Eve in case she guesses b correctly in this modified protocol.

6. *(4 points)* Show that a q-ary maximum distance separable $[n, k]$-code is equivalent to an orthogonal array $\mathrm{OA}(q, n, 1)$ of strength $n - d + 1$.