IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises IX.

1. *(4 points)* Consider Shamir's $(5, 3)$ threshold scheme with $p = 567997$.

   (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 for shares $(1, 64104)$, $(2, 156586)$, $(3, 291500)$.

2. *(3 points)* Your research group is working on a super-secret project. There are two professors, three post-docs, five Ph.D. students and two external consultants. Propose a secret sharing scheme such that at least:

   - one professor, or
   - three post-docs, or
   - two post-docs and two Ph.D. students, or
   - two post-docs, one Ph.D. student and two external consultants, or
   - one post-doc and four Ph.D. students

   have access to the research results.

3. *(3 points)* Alice, Bob and Charlie use the Blakley's secret sharing scheme. Their individual shares are the parametrized planes

   $$\begin{aligned} &(s + 1, 5s + 3t + 2, 2t + 3), \\ &(s + 1, -s - t + 2, t + 3), \\ &(3s + 1, 2s - t + 2, 3t + 3), \end{aligned}$$

   $s, t \in \mathbb{R}$, respectively. Find the shared secret.

4. *(4 points)* For the following orthogonal arrays either find such an array or prove that such cannot exist.

   (a) $\mathrm{OA}(2, 4, 1)$
   (b) $\mathrm{OA}(2, 6, 2)$

5. *(5 points)* Suppose that n users use Shamir's secret sharing schemes to share two secrets S and S' with the same threshold t and prime modulus p. Each user $1 \leq i \leq n$ has share $s_i = (i, y_i)$ and $s'_i = (i, y'_i)$ for the secrets S and S', respectively. Show that these two schemes can be used to easily (without revealing any information about their shares to anyone else) construct a third secret sharing scheme for the secret $S + S'$ and find the corresponding share for each user.

6. *(4 points)* 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 $v = \alpha^{-a} \equiv 47 \mod p$.

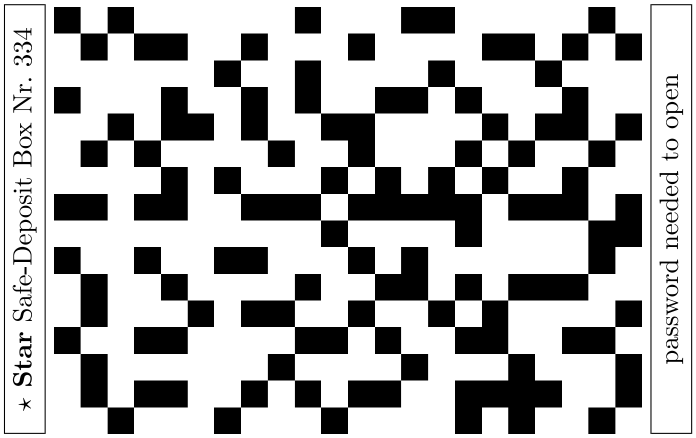
   (a) Which of the following is a transcript (γ, r, y) of a correctly performed execution of the Schnorr identification scheme? (There are multiple correct transcripts).

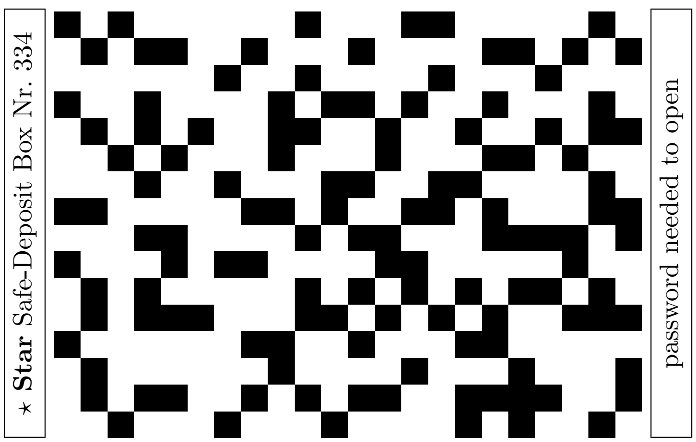
   $$(83, 21, 7), (83, 17, 21), (126, 19, 15), (126, 11, 8)$$

   (b) Use two of these valid transcripts to recover the secret key a, with the knowledge that instead of choosing new k at random for each run, Alice uses a pseudorandom update function $k_{i+1} = 3k_i + 4 \mod 31$.

More on next page >>>

7. *(3 points)* You have received the following card allowing you to open the safe-deposit box. It is clear that you need a password to open the box. Unfortunately, you do not know this password. At the same time, your colleague received a similar card for the same safe-deposit box...





8. *(4 points)* Consider the general form of orthogonal arrays:
A t-(n, k, λ) 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. Prove the following:

   (a) For all t and all n, there exists a t-$(n, t+1, 1)$ array.

   (b) If there exists a t-(n, k, λ) orthogonal array, then there exists a $(t-1)$-$(n, k-1, \lambda)$ orthogonal array.