IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises IX.

1. Consider the basic Fiat-Shamir identification scheme with secret keys $p = 61$, $q = 97$ and $s = 1972$. Calculate the following parts of the protocol:
   (a) Alice's commitment to Bob with random choice $r = 315$.
   (b) Alice's response to Bob's challenge $b = 1$.
   (c) Bob's verification of Alice's response to his challenge.

2. 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 for shares $(1, 122670), (2, 438907), (3, 450719)$.

3. Consider an orthogonal array $\mathrm{OA}(n, k, \lambda)$ as it was defined in the lecture. Such orthogonal array has strength $s = 2$, in any two columns of the array every one of the possible n^2 pairs of symbols occurs in exactly λ rows. Generally, for an orthogonal array of strength s, in any s columns of the array every one of the possible n^s ordered s-tuples of symbols occurs in exactly λ rows.

   Give an example of orthogonal array $\mathrm{OA}(2, 4, 1)$ of strength 3.

4. Show how to construct a $(k - 1, s)$-threshold secret sharing scheme from an orthogonal array $\mathrm{OA}(n, k, 1)$ of strength s.

5. Consider the password system that uses lowercase letters, uppercase letters and digits as character set and that uses a hash function producing an h-byte long hash. Passwords with a minimum length of 3 characters and a maximum length of 6 characters are allowed. Consider you want to pre-compute a dictionary that maps every possible password to its hash value. Assuming each character requires one byte what would be the required storage size for this dictionary if
   (a) unsalted passwords are used;
   (b) passwords with a 2 characters long salt that is randomly chosen from the character set consisting of lowercase letters are used.

6. Consider the following secret sharing scheme. Arthur, Barbara, Clark, Donald, Elisabeth and Fay – each is given a different piece of information about a secret natural number n:
   - Arthur knows that n is prime.
   - Barbara knows that the binary representation of n contains at most 11 digits.
   - Clark knows that $n \equiv 2 \pmod 5$.
   - Donald knows that $n \equiv 5 \pmod{503}$.
   - Elisabeth knows that the binary representation of n contains at least 11 digits.
   - Fay knows that n is a divisor of 60510.

   Find n and determine all possible combinations of persons who are able to determine the secret together with certainty.

7. Consider the Okamoto Identification Scheme (omit the digital signatures for simplification) with malicious Bob trying to reveal Alice's secret keys a_1, a_2, k_1 and k_2. Suppose Bob has a probabilistic polynomial time algorithm that allows him to do this. Show that in such case, he could use this algorithm to compute the discrete logarithm $\log_{\alpha_1} \alpha_2$.