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

1. *(3 points)* Use the Chinese reminder theorem to solve the following system of linear congruences (for $0 \leq x < 1309$):

$$\begin{aligned} x &\equiv 6 \pmod{17} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 9 \pmod{11} \end{aligned}$$

   Show computation steps in detail.

2. *(2 points)* Determine which of the numbers $1, \ldots, 10$ are quadratic residui modulo the prime 8009 without using brute force.

3. *(4 points)*

   (a) Encrypt your UČO (personal identification number) using the Rabin cryptosystem with $n = 698069$. Then calculate all four possible decryptions of the ciphertext you calculated, with the knowledge that $n = 887 \times 787$.

   (b) Encrypt your UČO with the ElGamal cryptosystem with $p = 567899$, $q = 2$, $x = 12345$ and random choice $r = 938$.

4. *(6 points)* Consider the following hash function $h(m)$:

   i. Choose a prime p such that $q = \frac{p-1}{2}$ is prime.

   ii. Choose primitive roots $\alpha, \beta \in \mathbb{Z}_p^*$.

   iii. The hash of a message $m = x + yq$ with $0 \leq x, y \leq q - 1$ is then defined as

$$h(m) = \alpha^x \beta^y \mod p.$$

   Show that finding two colliding messages $m \neq m'$ with $h(m) = h(m')$ is at least as hard as solving the discrete logarithm problem $\log_\alpha \beta \pmod{p}$.

5. *(5 points)* Consider a group of 5 people. What is the probability that

   (a) at least two

   (b) exactly two

   (c) at least three

   of them was born on the same day of the week?

   Assume that each day of the week (Monday, ..., Sunday) is equally likely as a birthday.

6. *(5 points)* Consider the Rabin cryptosystem with public key $n = pq$, where $p \equiv q \equiv 3 \mod 4$. Show that each of the four possible decryptions x_1, x_2, x_3, x_4 of ciphertext c, is uniquely determined by two bits of information – its parity ($x_i \mod 2$) and Jacobi symbol $\left(\frac{x_i}{n}\right) \in \{1, -1\}$. You can use properties of Jacobi symbol without proof.