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

1. *(3 points)* Sign your UČO using:
   (a) the RSA signature with $(d; e, n) = (303703; 7, 1065023)$
   (b) the ElGamal signature with $(x; q, p, y) = (60221; 2, 555557, 552508)$ and a random component $r = 12345$.
2. *(3 points)* Consider the RSA signature scheme with public key $(n, e) = (581, 17)$. Malicious Eve captured the following messages signed by Alice: $(m_1, sig(m_1)) = (33, 192)$, $(m_2, sig(m_2)) = (6, 454)$. Show that Eve can forge the signatures of messages $m_3 = 198$, $m_4 = 508$ and $m_5 = 97$ without using brute force.
3. *(3 points)* Consider the Ong-Schnorr-Shamir subliminal channel with $n = 29737$ and $k = 13$. Compute in detail the public key and the signature of the message $w' = 2020$ containing the secret subliminal message $w = 111$. Demonstrate that the signature is valid and that the secret message can be recovered.
4. *(4 points)* Consider the following (t, n) threshold signature scheme based on RSA signatures:
   (a) A trusted dealer T selects an RSA modulus N with keys e and d, makes (N, e) public.
   (b) T gives every party i of the threshold scheme a secret share d_i, such that $d = d_1 + d_2 + \ldots + d_n$.
   (c) To sign a message m every party i first computes partial signature $s_i = m^{d_i} \mod N$.

   Find (and prove its correctness) the final step of the scheme so that the parties can together obtain the signature $s = m^d \mod N$ of the message m. What are the possible t (in terms of n) for which this scheme is correct?
5. *(5 points)* Consider the Lamport one-time signature scheme for signing a 4-bit message, ie. the signer creates a list of private keys y_{ij} and publishes the corresponding public keys z_{ij}, $1 \leq i \leq 4$, $0 \leq j \leq 1$. Is it possible to securely sign any 6-bit message with such scheme? Explain your answer.
6. *(7 points)* At the end of the semester Professor Gruska regularly receives a list of 5 students with the highest achieved points for homework exercises, so that he can award them with final mark A. This takes the following form:

   $$\begin{array}{c} \text{UČO}_1,\ sig(\text{UČO}_1) \\ \text{UČO}_2,\ sig(\text{UČO}_2) \\ \text{UČO}_3,\ sig(\text{UČO}_3) \\ \text{UČO}_4,\ sig(\text{UČO}_4) \\ \text{UČO}_5,\ sig(\text{UČO}_5) \end{array}$$

   In order to protect this list from being tampered with, the ElGamal signature with public information $(q, p, y) = (2, 567899, 300210)$ was used. You have intercepted the following list:

   $$\begin{array}{l} 172459, (226741, 13448) \\ 172519, (331901, 326010) \\ 359406, (390725, 78981) \\ 456149, (144902, 184381) \\ 459379, (43870, 540485) \end{array}$$

   Additionally, you have learned that in order to save on randomness, the signatures were calculated with r_1, r_2, r_3, r_4, r_5, where for all $i \in \{2, 3, 4, 5\}, r_i = 3 * r_{i-1} \mod 567898$. Without using brute force, modify the list such that it contains your signed UČO. Explain your answer.