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

1. *(2 points)* Sign your UČO using the following signature scheme and verify the signature:
   (a) the RSA signature scheme with $(d, e, n) = (303703; 7, 1065023)$
   (b) the ElGamal signature scheme with $(x, q, p, y) = (60221; 2, 555557, 552508)$ and a random component $r = 12345$.

2. *(7 points)* Consider the ElGamal signature scheme.
   (a) Show that the scheme is vulnerable to existential forgery. Show that an adversary can produce a combination of message w and a correct signature (a, b), but cannot choose the value of w.
   (b) Show that given a valid signature (a, b) of a message w, an adversary can compute signatures for messages of the form $w' = (w + \beta b)\alpha \mod (p-1)$, for an arbitrarily chosen $\beta \in \mathbb{Z}_p^*$ and $\alpha = q^\beta \mod p$.
   (c) Show that if the signer chooses the same r to sign two messages w_1 and w_2, the private key x can be computed.

3. *(4 points)* Consider the Ong-Schnorr-Shamir subliminal channel with $n = 3431$ and $k = 20$. Compute in detail a signature of the message $w' = 122$ which contains the secret subliminal message $w = 108$. Demonstrate that the calculated signature is valid and that the secret message can be recovered.

4. *(4 points)* Consider Chaum's blind signature scheme with the public key ($n = 10033$, $e = 101$) and the private key $d = 1265$. Describe in detail blinding, signing, and unblinding actions as well as verification of the obtained signature of message $m = 1234$ using random $k = 8824$.

5. *(3 points)* Use the Lamport one-time signature scheme to sign 4-bit messages with $f(y) = 17^y \mod 61$ and the following secret keys y_{ij}, $1 \le i \le 4$, $j = 0, 1$:

i	1	2	3	4
y_{i0}	7	37	31	47
y_{i1}	4	36	55	11

   (a) Compute the public keys z_{ij}.
   (b) Sign the message 0111 and then verify the signature.
   (c) Verify the signature $(4, 37, 31, 11)$ of the message 1001 using your computed public keys.

6. *(4 points)* Bob is using a single RSA scheme to both decrypt encrypted messages and create signatures (with the same set of public and private keys). You have intercepted an encrypted message c directed at Bob. Use his signature scheme to make him help with decryption of c without him being able to realize he is helping you.

7. *(6 points)* Consider the following signature scheme. Choose primes p, q such that $q \mid p-1$. Choose a generator $g \in \mathbb{Z}_p^*$ of order q. Choose a random $x \in \mathbb{Z}_q^*$ and compute $y = g^x \mod p$. The value x serves as a secret key, while p, q, g and y are public.

   To sign a message m, choose a random $k \in \mathbb{Z}_q^*$ and compute $r = g^k \mod p$ and $s = k - H(m||r)x \mod q$ where $H : \{0,1\}^* \to \mathbb{Z}_q$ is a cryptographic hash function. The pair (r, s) is the signature of m.

   (a) Provide a verification procedure for the proposed scheme and prove that it is correct.
   (b) Show that a private key x can be recovered if the same k is reused.