IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises VII.

1. Sign your UČO using:
   (a) RSA signature with $(d; e, n) = (303703; 7, 1065023)$
   (b) ElGamal signature with $(x; q, p, y) = (60221; 3, 555557, 214441)$ and random $r = 12345$.

2. Consider the Ong-Schnorr-Shamir subliminal channel with public key $n = 2018$, $h = 113$ and the trapdoor information $k = 77$. Compute in detail signature of the message $w' = 133$ which contains secret subliminal message $w = 27$. Show that the signature is valid and that the secret message can be recovered.

3. Consider Chaum's blind signature scheme, with public key $n = 2183, e = 17$ and private key $d = 737$. Alice wants Bob to sign message $m = 13$ blindly. Describe in detail signing and verification with random secret $k = 25$.

4. Show that if the signer chooses r in the ElGamal signature scheme randomly, and then increments it by two (assume $r + 2$ is invertible modulo $p - 1$) to sign another message, then given these two ElGamal signatures (on two different messages m_1 and m_2), the private key x can be computed.

5. Consider the Lamport signature scheme with one-way function

$$f(y) = 44^y \mod 71$$

   and the following public key:

i	1	2	3	4	5
z_{i0}	23	50	4	16	28
z_{i1}	25	42	45	64	11

   Verify the signature $(42, 61, 54, 22, 41)$ of message 11010.

6. ElGamal signature scheme with public key $(p, q, y) = (97, 10, 7)$ was used to sign messages $w_1 = 54$ and $w_2 = 13$ with $sig(w_1) = (40, 38)$ and $sig(w_2) = (40, 25)$. Without calculating the discrete logarithm or using other kind of brute force, find the secret key x.

7. Consider Alice and Bob use the DSA signature scheme with $p = 2347$, $q = 23$, $r = 266$, $x = 11$ and $y = 864$. Alice signs $w = 1000$ and sends the corresponding signature $sig(w) = (7, 20)$ to Bob. Surprisingly, Bob shares with Alice her secret key x and his purpose is not only verification of the signature. Is Alice trying to communicate something to Bob?

8. Consider the ElGamal signature scheme with $p = 1117, q = 2, y = 925$. You have obtained message $w = 111$ with the signature $(a, b) = (178, 747)$. Find at least two other messages and their valid signatures without computing the private key or using brute force.

9. Alice and Bob used the Lamport signature scheme. Alice sent Bob two random signed messages of length n, but she used the same keys to sign both messages. Eve intercepted their communication. What is the expected number of messages of length n for which Eve knows the valid signature?