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

1. Consider Chaum's blind signature scheme with public key $(n, e) = (2279, 1135)$ and private key $d = 127$. Compute the signature of the message $m = 935$ using the random integer $k = 554$. Verify that the signature is the same as if the message was signed with the private key directly.

2. Consider the RSA signature scheme with public key $n = 96427$ and $e = 79$. You want to obtain the signature for the message $m = 14879$ and you are given one pick of any message $m' \neq m$ for which you will receive the corresponding signature. Which m' would you pick? Explain your reasoning.

3. Consider the ElGamal signature scheme with $p = 1367$, $q = 2$ and the public key $y = 307$. Suppose that you know the signature $(a, b) = (652, 945)$ for the message $w = 137$. Without computing the private key x, find a valid message-signature pair for a message $w' \neq w$. Explain your reasoning.

4. Consider the Diffie-Hellman key exchange protocol with $p > 5$ a safe prime, *i.e.* there exists a prime r such that $p = 2r + 1$. Let q be a primitive root modulo p. Suppose that Alice and Bob both choose their secret exponents x, y uniformly in the range $1 \leq x, y \leq p - 2$. Calculate the probability that the shared secret $q^{xy} \mod p$ is equal to 1.

5. Alice and Bob use the RSA signature scheme. Alice's public key is $(n, e) = (1333, 41)$. Suppose you have captured two signed messages sent by Alice: $(m_1, \mathrm{sig}(m_1)) = (314, 655)$ and $(m_2, \mathrm{sig}(m_2)) = (271, 612)$. Without factoring n, find a signature for the message $m_3 = 1162$. Verify that it is valid.

6. Sign your UČO (Personal identification number) using the following signature scheme:
   (a) RSA signature with $(d, e, n) = (303703, 7, 1065023)$.
   (b) ElGamal signature with $(x, q, p, y) = (60221, 3, 555557, 214441)$ and a random component $r = 12345$.
   (c) DSA signature with $(p, q, r, x, y) = (585199, 10837, 46053, 1337, 187323)$ and a random component $k = 8348$.

7. Bob uses the Lamport signature scheme but he wants to save time so he recycles his private keys in the following way. He chooses two permutations σ_0 and σ_1 of the set $\{1, \ldots, k\}$ and computes the new private keys $y'_{i,j}$ from the old private keys $y_{i,j}$ in the following way, for $1 \leq i \leq k$:

   $$y'_{i,j} = y_{\sigma_j^{-1}(i),j}$$

   He used his old scheme to sign the message $x_1 \ldots x_k$. When are you able to sign a whole message using his new scheme? What is this message?