IV054 Coding, Cryptography and Cryptographic Protocols
2011 - Exercises VII.

1. Find all integers a such that a is order of some element of the group $(\mathbb{Z}_{151}^*, \cdot)$.

2. Consider the ElGamal signature scheme. Let (p, q, y) be a public key and let x be a secret key.
   Let i, j be integers and $\gcd(j, p-1) = 1$.
   Let (a, b), where $a = q^i y^j \bmod p$ and $b = -aj^{-1} \bmod (p-1)$, be a valid signature for a message w.

   (a) Find w.

   (b) What can bad Eve do using this knowledge?

3. Alice and Bob use the Ong-Schnorr-Shamir subliminal channel with the public key $n = 2011$, $h = 1974$ and the trapdoor information $k = 171$. Demonstrate usage of the subliminal change on the secret message $w = 18$ and the harmless message $w' = 23$.

4. Alice use the DSA signature scheme to sign her messages. Her public key is $p = 877$, $q = 73$ and $r = 588$. Alice sent message $m_A = 55$ to Bob signed with the signature $(72, 0)$. Eve intercepted the message and wants to change it to $m_E = 50$ and forge Alice's signature. Perform all steps of her calculation and all steps of Bob's verification of a forged signature. Do not use brute force.

5. Consider the DSA signature algorithm with a hash function H. If H is not collision resistant, show that we can forge a given signature with a chosen-message attack. Apply this attack to SHA-1 by using brute force. What is its complexity?

6. Consider the following one-time signature scheme used for signing of N-bit messages.
   Let H be a cryptographically secure hash function.

   - (Initial phase) Alice chooses two random numbers x_1 and x_2 and computes $y_1 = H^M(x_1)$ and $y_2 = H^M(x_2)$ where $M = 2^N$. Alice publishes y_1 and y_2.
   - (Signing) Alice computes $s_1 = H^n(x_1)$ and $s_2 = H^{M-n-1}(x_2)$, where $0 \leq n \leq 2^N - 1$ is the value of an N-bit message to be signed.
   - (Verification) To verify a signature, Bob checks validity of the following equations:

   $$y_1 = H^{M-n}(s_1) \text{ and } y_2 = H^{n+1}(s_2).$$

   (a) Demonstrate usage of the proposed scheme on signing of 2-bit message '11'.

   (b) Explain why it is insufficient to compute only a value of s_1.

   (c) Compare the proposed scheme with Lamport one-time signatures.