2007 - Exercises VII.

1. Without computing a private key, give a valid message-signature pair for the following signature schemes. You are given only a public key.

   (a) the ElGamal signature scheme with $p = 2357$, $q = 2$ and $y = 1185$.

   (b) the RSA signature scheme $n = 3233$ and $e = 17$.

2. Suppose that Alice has signed two different messages using the ElGamal signature scheme and that she used the same r. Show that it is possible to find her private key with high probability.

3. Show how you can totally break the DSA signature scheme if you are given a signature $(a, 0)$ for a message w.

4. How would be the security of the ElGamal signature scheme affected if one would accept signatures (a, b) with a larger than p?

5. Consider the Lamport one-time signature scheme. A signer has signed m $(2 \leq m \leq 2^k - 1)$ different k-bit messages (instead of only one message he was allowed to sign). How many new messages an adversary would be able to forge?

6. Demonstrate the usage of the subliminal channel with $n = 4568$, $k = 3465$ and $h = 913$, a harmless message $w' = 15$ and a secret message $w = 9$.

7. Consider the Fiat-Shamir signature scheme. What happens if an adversary is able to find random integers $r_1, \dots, r_t$?

8. Let $n \in \mathbb{Z}$, $a, b \in \mathbb{Z}_n$ such that $\gcd(a, n) = d > 1$. Show that the equation $ax \equiv b \bmod n$ has no solution if d does not divide b and has d mutually different solutions otherwise.