IV054 Coding, Cryptography and Cryptographic Protocols
2016 - Exercises VII.

1. Alice is using the RSA signature scheme with public key $(n, e) = (581, 17)$. Malicious Eve captured two signed messages sent by Alice: $(m_1, sig(m_1)) = (15, 85)$, $(m_2, sig(m_2)) = (8, 281)$. Show that Eve can forge the signatures of messages $m_3 = 218$ and $m_4 = 120$ without using brute force.

2. Consider the ElGamal signature scheme with $p = 97$, $q = 10$, $y = 19$. You have received two messages $m_1 = 33$, $m_2 = 44$ with the following signatures $sig(m_1) = (37, 42)$, $sig(m_2) = (37, 61)$. Calculate valid signature for the message $m_3 = 57$.

3. Consider the Lamport signature scheme with $k = 4$, one way function $f(y) = y^2 \pmod{119}$ and the following secret keys y_{ij}, $1 \leq i \leq 4$, $j \in \{0, 1\}$:

i	1	2	3	4
y_{i0}	56	90	58	53
y_{i1}	6	30	63	86

   (a) Compute the public keys z_{ij}.

   (b) Sing the message 0011.

4. Suppose that you want an authority A that is using the RSA signature scheme to sign a message m but you do not want A to know m. How would you obtain A's signature of m without revealing the value of m to A?

5. Consider the ElGamal signature scheme where b is computed as

$$b = r^{-1}(a - xw) \pmod{(p-1)}.$$

   Find the verification equation and prove that it works.

6. Find a way to use Rabin signatures as a subliminal channel that allows Alice to send at least two secret bits to Bob with every signed message. This channel must look like a normal channel with Rabin signatures to the warden Walter who must not be able to retrieve the secret message.

7. Consider the Merkle trees. Show that if one can find two trees with the same value assigned to the root node but with different values assigned to leafs then one can find a collision in the underlying hash function.