IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises VII.

1. Let m be a message which the adversary Eve intends to sign using the RSA signature scheme with a public key (n, e) and a private key d. Suppose that Eve can obtain a signature of any message $m' \neq m$. Show that this enables her to sign m.

2. Consider the RSA signature scheme with public key $(n, e) = (1927, 1483)$. Verify signatures s_i of messages w_i.

   (a) $w_1 = 11$, $s_1 = 416$;

   (b) $w_2 = 123$, $s_2 = 1477$;

   (c) $w_3 = 56$, $s_3 = 200$.

3. Consider the following signature scheme. Alice has a public key (p, g, X, Y), where $p \geq 3$ is a prime, g is a generator of $(\mathbb{Z}_p^*, \cdot)$, $X = g^x \pmod{p}$ and $Y = g^y \pmod{p}$, and a private key (x, y) where $x, y \in \mathbb{Z}_p^*$. The signature of a message m is $s = y + xm \pmod{p}$. Find a verification algorithm for this scheme and show its correctness.

4. Suppose Alice uses the Fiat-Shamir signature scheme with $v_1 = 6003, v_2 = 1919, v_3 = 2980$, $s_1 = 44, s_2 = 45, s_3 = 46$, $h(x) = x \bmod 2011$ and $n = 7223$.
   Show in detail the computation steps of signing message 33 with $r_1 = 1200, r_2 = 2400, r_3 = 3600$.

5. Consider the DSA signature scheme with a hash function H. If H is not one-way, show that we can forge a triplet $(m,\, a,\, b)$ such that $(a,\, b)$ is valid signature for the message m.

6. Consider the DSA signature scheme. Let (p, q, r, x, y) be a key. Suppose the public parameters

$$p = 48731, \quad q = 443, \quad \text{and} \quad r = 5260.$$

   The element r was computed as $r \equiv 7^{48730/443} \pmod{48731}$, where 7 is a primitive root modulo 48731. Alice chooses the secret signing key $x = 242$.

   (a) What is Alice's public verification key y?

   (b) Alice signs the message $m = 343$ using $k = 427$. What is the signature? Perform all steps of her calculation and all steps of Bob's verification.

7. Let n be a large composite modulus (of unknown factorization), k and s be two elements of $\mathbb{Z}_n^*$ such that $s^2 = -k \pmod{n}$. Let $H : \{0,1\}^* \to \mathbb{Z}_n$ be a cryptographic hash function. Find a signature algorithm which uses the public key k, the secret key s if you know that the verification of a signature (x, y) of a message m consists in checking that

$$x^2 + ky^2 \equiv H(m) \pmod{n}.$$