IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises VII.

1. Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a one-way function. Find a one-way function f' for which the Lamport signature scheme does not have the following property. For any message m and a valid signature s for m, it is infeasible to find a pair $(m', s') \neq (m, s)$ such that s' is a valid signature for m'.

2. Use the Ong-Schnorr-Shamir subliminal channel scheme with $n = 5617$ and $k = 111$ to verify and decrypt the message $(w', S_1, S_2) = (1234, 3058, 4806)$.

3. Consider the following signature scheme. Let q be a large prime, g a generator of the group $\mathbb{Z}_q^*$ and h a proper (publicly known) hash function. Alice's private key is an integer $x \in \{1, 2, \ldots, q-1\}$ and her public key is $y = g^x \pmod{q}$. Alice signs a message m by computing $g^z \pmod{q}$ where $z = \frac{x}{h(m)} \pmod{q}$ (we require that $h(m) \neq 0 \pmod{q}$).
Alice's signature s is accepted if $s^{h(m)} = y \pmod{q}$. Decide whether the described signature scheme is correct and secure. Explain your reasoning.

4. Alice is using the DSA scheme for signing her messages. She has the following public key: $p = 3583$, $q = 199$ and $r = 1614$. Alice has sent a message $m = 46$ with signature $(102, 0)$. Malicious Eve has intercepted the message and she wants to change the message to $m' = 50$ so that Bob will not find it. Find a valid signature for $m' = 50$ (do not use brute force attack) and verify it. Explain your answer.

5. Suppose that there is a web service which offers its users on-line computation of discrete logarithms for any cyclic group and its generator. Alice needs to compute a discrete logarithm of $a \in G$ in basis $g \in G$ where G is a cyclic group. She would like to use the web service but she does not want to give it any information about a. Decide whether there is a way for Alice to achieve her goal.

6. Let us consider the Chaum's blind signature RSA scheme with $n = pq$, $p = 71$, $q = 83$, $e = 31$. Only Bob knows d and he uses it to sign documents. Alice wants him to sign message $m = 2431$ without him knowing m. Compute in detail a signature for m with $k = 128$.

7. Consider the DSA signature algorithm with public key p, q, r and a secret key x. Suppose a lazy signer has precomputed one pair (k, a), satisfying $a = (r^k \bmod p) \bmod q$, and uses the same pair for each signature. Show how to recover his secret key.