Introduction to Cryptography

Homework 3

Submission date: 26.12.2004
Exercises submitted on 19.12.2004 will receive a 5 point bonus.

1. This question shows that the El Gamal signature scheme is insecure if the signer does not use a new k for every signature.
    - If the same value of k is used for signing m_1 and m_2, then $s_1 = (m_1 - ar)k^{-1} \bmod p\text{-}1$, and $s_2 = (m_2 - ar)k^{-1} \bmod p\text{-}1$.
    - Then, $(s_1 - s_2)k = (m_1 - m_2) \bmod p\text{-}1$.

    a. Show that if $s_1 - s_2 \neq 0 \bmod p\text{-}1$, then k can be easily found.
    (Note that $\gcd(s_1 - s_2, p\text{-}1)$ might be different from 1. You will get a 5 point bonus for handling this case.)

    b. Show that if k is known, then the secret key can be easily found.

2. This question shows that the El Gamal signature scheme is insecure if the verifier does not check that $r < p$.

    Let (r, s) be a signature on a message m.
    The adversary can compute a signature on an arbitrary message m' as follows:
    - Set $u = m' \cdot m^{-1} \bmod p\text{-}1$.
    - Set $s' = s \cdot u \bmod p\text{-}1$.
    - Compute r' satisfying
        - $r' = r \cdot u \bmod p\text{-}1$.
        - $r' = r \bmod p$.

    The signature of m' is (r', s').

    a. How is r' computed and what is the range of its possible values?
    b. Show that (r', s') is a valid signature of m'.