IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises VII.

1. Suppose that the ElGamal signature scheme is used and that signatures in which either $a = 0$ or $b = 0$ are allowed. Show that such scheme is not secure.

2. Let (n, e) be a public key for the RSA signature scheme. Suppose that there is an efficient algorithm A which is able to compute valid signatures for this public key for a small fraction of possible messages without the corresponding private key d. More precisely, it holds that $\frac{|S|}{|\mathbb{Z}_n^*|} = 0.01$ where $S \subset \mathbb{Z}_n^*$ is a set of all messages for which A returns a valid signature.

   Show that A can be used to compute a valid signature for any possible message with high probability. You are supposed to propose a randomized algorithm.

3. Consider the DSA signature scheme with $p = 7879$, $q = 101$, $h = 170$ and $x = 75$. Compute in detail a signature of a plaintext 5001 using $k = 4$ and show that your signature is valid.

4. Consider a modification of the RSA signature scheme in which a signature s for a message m is computed as

   $$s = (0||m||0^{\frac{l}{10}})^d \pmod{n},$$

   where $||$ denotes a concatenation of bit strings and l is length (number of bits) of n.

   Show that this signature scheme is not secure.

5. Show that using the same k to sign two messages allows the DSA scheme to be broken.

6. Consider a modification of the ElGamal signature scheme in which $x \in \mathbb{Z}_{p-1}^*$ and b is computed as

   $$b = (w - ra)x^{-1} \pmod{(p-1)}.$$

   Describe how verification of a signature (a, b) on a message x would proceed.

7. Alice and Bob became annoyed with using both digital signatures and encryption in order to ensure data authentication and confidentiality. They decided to sign and encrypt messages at once using the following "signcryption" scheme.

   - All messages have a fixed length l, Alice has a public key (e_A, n_A) and a private key d_A and Bob has a public key (e_B, n_B) and a private key d_B. The keys are defined in the same way as in the RSA cryptosystem and both moduli are of size k bits.
   - Further, $k = l + k_0 + k_1$ where $k_0, k_1 > 0$ are small integers.
   - Finally, Alice and Bob agreed on hash functions $g : \{0,1\}^{k_1} \to \{0,1\}^{l+k_0}$ and $h : \{0,1\}^{l+k_0} \to \{0,1\}^{k_1}$.

   To signcrypt a message m for Alice, Bob performs the following steps:

   (1) Choose a random number r of size k_0 bits.
   (2) Compute $w = h(m||r)$.
   (3) Compute $v = g(w) \oplus (m||r)$.
   (4) If $(v||w) > n_B$, return to the first step.
   (5) Compute $s = (v||w)^{d_B} \pmod{n_B}$.
   (6) If $s > n_A$, put $s = s - 2^{k-1}$.
   (7) Compute $c = s^{e_A} \pmod{n_A}$.
   (8) Send c to Alice.

   Describe in detail Alice's steps after she receives a bit string b of size k bits which is supposed to be a signcrypted message from Bob. The result should be either rejection or acceptance in which case the original message should be recovered. Explain the steps.