Wrocław University of Technology, WPPT 13.11.07

CRYPTOGRAPHY AND SECURITY, 2007 Assignments, list # 5

1. Design as many as possible "ElGamal-like" digital signature schemes. For each case present appropriate verification test.

2. If no hash function is used, then ElGamal signatures can be forged. Indeed, select u, v such that $gcd(v, p-1) = 1$. Let

   $$r := g^u y^v \bmod p, \quad s := -rv^{-1} \bmod p-1$$

   Show that (r, s) is a valid signature for $m = su \bmod p-1$.
   How the use of a hashing function prevents such an attack?

3. Bilinear mappings can be used to design ID-based signature schemes. ID-based means that the public key can be derived directly from the ID of the signer. The following scheme implements this idea: s is a system wide secret, and $Q_{pub} = sQ$ is the public parameter. For a user with identity R the private key is

   $$S_R := \frac{1}{H_1(R) + s} P$$

   (H_1 is a hashing function). Signing procedure is as follows

   (a) choose k at random and compute $r := g^k \bmod p$,

   (b) $h := H_2(M, r)$, where M is the message to be signed.

   (c) compute $S := (k + h)S_R$

   Show that the following test is a sound verification procedure:

   $$h = H_2(M, e(S, H_1(R)Q + Q_{pub})g^{?h})?$$

4. For an RSA number $n = pq$, what is the probability that a number $a < n$ chosen at random has exactly two square roots?

5. Design a blind RSA signature scheme - a scheme such that the signer creates the signature of m without knowing m. The scheme works as follows:

   (a) Alice creates a message $f(m)$ and gives it to Signer,

   (b) Signer encrypts $f(m)$ with his secret key,

   (c) Alice transforms the cipertext to a ciphertext of m.

   How to design such a scheme - find f and a transformation scheme?

/-/ Mirosław Kutyłowski