Wrocław University of Technology, WPPT 25.11.09

CRYPTOGRAPHY AND SECURITY, 2009 Assignments, list # 6

1. Consider the rho-Pollard method for computing discrete logarithms. During its execution we get c, d such that $\alpha^c = \beta^d \bmod p$.

   - How to reduce the probability that $GCD(d, p-1) > 1$?
   - What to do if $GCD(d, p-1) > 1$? Do we really have to start from scratch?

2. Design alternative digital signature systems similar to ElGamal with different test algorithms.

3. Propose some methods to protect ElGamal encryption from changing the plaintext of the ciphertext.

4. It is possible to re-encrypt an ElGamal ciphertext. Namely, if we are given $(a, b) = (\beta^k \cdot m, g^k)$ then we can compute $(a, b) := (a \cdot \beta^r, b \cdot g^r)$ as a new ciphertext of m.

   Show that it is possible to design an ElGamal-like encryption scheme that makes it possible to re-encrypt without knowing the public key used.

5. Find Polish legal rules concerning requirements for advanced electronic signatures (*bezpieczny podpis elektroniczny weryfikowany kwalifikowanym certyfikatem*). That is: *Ustawa o podpisie elektronicznym* from 2001, and *Rozporządzenie Rady Ministrów 1094* from 2002.
   Design implementation details of DSA-like scheme so that all requirements are fulfilled, but the solution is totally insecure.

/-/ Mirosław Kutyłowski and Filip Zagórski