Wrocław University of Technology, WPPT 15.12.09

CRYPTOGRAPHY AND SECURITY, 2009 Assignments, list # 7

1. Estimate the expected runtime of factorization on an RSA number $n = pq$ with the rho-Pollard algorithm.

2. Show that is p is a prime number, then the number of square roots of a, for $0 < a < p$, is either 2 or 0.
   Given an RSA number $n = pq$ and $a < n$. How many square roots of a modulo n may exist?

3. Let n be an RSA number. Let $k > 2$, and $a < n$ with gcd$(a, n) = 1$. What is the number of roots of a of degree k?

4. ElGamal encryption algorithm can be implemented for $\mathbb{Z}_n$, where n is an RSA number, instead of $\mathbb{Z}_p$ for a prime p.

   Is it secure?

5. Present details of breaking RSA ciphertexts based on an oracle providing the least significant bit of the plaintext corresponding to the input RSA ciphertext.

6. Consider the following setting for Rabin scheme: p and q are distinct primes, $p, q = 3 \bmod 4$, $n = pq$. Show that:

   - If GCD$(x, n) = 1$, then $x^{(p-1)(q-1)/2} = 1 \bmod n$,
   - If x is a square modulo n, then $x^{(n-p-q+5)/8} \bmod n$ is a square root of x modulo n.

/-/ Mirosław Kutyłowski and Filip Zagórski