Wrocław University of Technology, WPPT 22.11.07

CRYPTOGRAPHY AND SECURITY, 2007 Assignments, list # 6

1. Why factorization based on factor base method is not sufficient enough to break RSA?
2. Estimate the expected runtime of factorization on an RSA number $n = pq$ with the rho-Pollard algorithm.
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. Consider the factorization method of n based on knowledge of a pair of RSA keys e, d. What is the probability of success in a single iteration with an a chosen at random?
5. 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?

/-/ Mirosław Kutyłowski