Wrocław University of Technology, WPPT 19.10.02

Cryptography, 2004 Assignments, list # 2

1. Binary gcd algorithm is based on binary representation. Does it make sense to base it on other representations? Consider the case when we examine divisibility by 4. Implement necessary changes in the algorithm (write down a pseudocode) and determine efficiency of such a solution.
2. Estimate the number of $k < n$ such that k has at least one divisor less than B. Based on this estimation discuss how much influence on the runtime of primality test has preliminary trial divisions by small prime numbers.
3. Let n be a RSA number. Let $e < \phi(n)$ be arbitrary. Given $a < n$. How many roots of degree e of a exist? Discuss all cases.
4. Estimate the probability that Miller-Rabin primality test finds an appropriate witness for an RSA number n (i.e. a witness that proves n to be composite).
5. estimate probability that Pollard rho algorithm for factoring $n = pq$ succeeds in one iteration given that p is B-smooth.
6. RSA operations with the public exponent should be as simple as possible. However, we do not like to use the public exponent e due to attack based on the trick of computing m^3 when three different users get the same text m. What solutions would you propose?
7. Consider the tasks of computing $m^e \bmod n$ for a fixed parameter e. Assume that the binary representation of e contains only a few ones. Which exponentiation algorithm is best suited for this case?

/-/ Mirosław Kutyłowski