Philadelphia University

Department of Basic Sciences

Exam 1 **Computational Number Theory** **24–03–2009**

1. Given that $1187^2 \equiv 632^2 \pmod{3959}$. Factor the number 3959 by computing GCD using the Euclidean algorithm.
2. In RSA, Alia selects $n = 319$ and $e = 19$. If the intended message is $m = 66$, compute $s = m^e \,\%\, n$ using successive squaring algorithm.
3. In RSA, suppose that $n = 11371$ and it is known that $\phi(n) = 11152$. Factor n using the quadratic formula.
4. Illustrate Fermat factorization using the number $n = 12533$
5. Write $n = 10t + u$. Prove that $19 \mid n$ if and only if $19 \mid t + 2u$.

–Amin Witno