Philadelphia University

Department of Basic Sciences

Final Exam **Computational Number Theory** **22–01–2012**

1. For RSA, let $n = 7 \times 29$ and $e = 5$. If $s = 123$, find m.
2. Factor $n = 2041$ using Quadratic Sieve with $46 \leq x \leq 51$ and $p \in \{2, 3, 5, 7\}$.
3. The number $n = 2^{2^7} + 1$ is composite. Is n a Fermat pseudoprime base $a = 2$? Why or why not?
4. Apply Miller-Rabin test for $n = 3281$ with $a = 3$. Which one is your conclusion? (a) prime (b) composite (c) pseudoprime (d) no conclusion
5. Apply Lucas primality test for $n = 761$ with $a = 7$. Which one is your conclusion? (a) prime (b) composite (c) pseudoprime (d) no conclusion

–Amin Witno