MATH 3375 (Theory of Cryptology) – Fall 2013

Homework Assignment 8

Due: Nov. 19, 2013

---

1. From Section 4.2 Exercise 1, 3, 5.
2. Suppose a public key of $(e, n) = (1093, 2747)$ is given. Encrypt the word `MATHEMATICS`. As in class, break the message into letters of size two, i.e., MA, TH, etc. Associate A with 01, B with 02, and so on. For the filler (since the message has 11 letters), use 00.
3. Download a copy of the original paper of Rivest, Shamir, and Adlerman (a copy can be found on the class website) on RSA cryptography.
   (*i*) Suppose $p = 2017$ and $q = 3109$. According to Section VII, Part C, what would be a good choice for d? Find such a d. (Note: answer is not unique!)
   (*ii*) Read Section IX on security. Explain why if one could compute $\phi(n)$ easily, one can also factor n easily. Illustrate your answer using the fact that $\phi(2773) = 2668$.