MATH 342—Homework problems on RSA

June 9, 2006

(1) Compute the greatest common divisor of 2668 and 157, and find integers a and b such that $2668a + 157b$ equals that greatest common divisor. Compare to the computation at the beginning of section VIII of the RSA paper.

(2) What is the remainder when 365^{365} is divided by 101?

(3) If the RSA modulus is $n = 5767$ and the encryption exponent is $e = 119$, find the decryption exponent d. (Hint: notice that $5767 + 9 = 5776$, which is the same as $5767 + 3^2 = 76^2$. Does this help you factor n?)

(4) Using RSA encryption with $n = 33$ and $e = 7$, encrypt the message `CODE`.

(5) The ciphertext `16 2 16 2 20` was encrypted using RSA encryption with $n = 33$ and $e = 7$. Find the plaintext message.