

Math 115B Midterm -Winter 2009

Due in class at 12:35pm, February 18, 2009. You are to work on your own, and may only consult your notes, text or the class web page. It is important that you write up your work in a clear and legible fashion.

1. Prove that for any integer n , n^5 and n have the same final digit.
2. Find primes p and q such that $n = pq = 6059$ and $\varphi(n) = 5904$. In general, explain why knowledge of n and $\varphi(n)$ allows one to factor n when n is a product of 2 primes.
3. Suppose that a cryptanalyst discovers a message m , $0 < m < n$, that is not relatively prime to the modulus $n = pq$ used in a RSA cipher system. Explain why the cryptanalyst can now break the code by factoring n .

In the following problems, encryption is done using the “standard alphabet equivalents”: $a \leftrightarrow 00$, $b \leftrightarrow 01$, \dots , $z \leftrightarrow 25 \pmod{26}$. (In actual practice, one usually starts with $a \leftrightarrow 01$, in order to avoid having “a” always encipher as 00.)

4. A Hill (Block) cipher using a 2×2 matrix produces the ciphertext 06 25 18 02 23 13 21 02 10 06 05 17 21 23. You know that the plaintext message begins with “THE” and ends in “EX”. Cryptanalyze (decipher) this message.
5. What are the first 6 digits of the ciphertext of the message “bestwishes” when the RSA cryptosystem with key $(e, n) = (5, 2669)$ is used with digraphs (i.e., $be\ st\ wi\ sh\ es \leftrightarrow 0104\ 1819 \dots$).
6. Cryptanalyze (decipher) the ciphertext 2206 0755 0436 1165 1737 received from someone using an RSA cryptosystem with public key $(e, n) = (13, 2747)$.
7. Prove that 2 is a primitive root for $p = 29$. Find all of the primitive roots for $p = 29$. Explain carefully how you accomplished this.
8. Selecting the primitive root $\alpha = 2$ for $p = 29$, Bob makes public his key $(p, \alpha, \beta) = (29, 2, 20)$ for communication using an El Gamal public key cryptosystem. Alice wishes to send Bob the message “call me”. She chooses her secret integer k and sends the key $r = \alpha^k = 8$ to Bob as well as the encrypted letters $(t_1\ t_2\ t_3\ t_4\ t_5\ t_6) = (21\ 00\ 14\ 14\ 10\ 13)$. Help Bob to decrypt her message. (Not a realistic example!)
9. Use discrete logarithms to find all solutions to the congruences $3x^5 \equiv 1 \pmod{29}$ and $3^x \equiv 2 \pmod{29}$.
10. Why is $X^4 + X + 1$ irreducible in $\mathbb{Z}_2[X]$? Use this fact or any other method to construct a field with 16 elements. Exhibit at least one primitive element for this field (i.e. an element that generates all non-zero elements of the field).