MCS 425: Codes and Crytography

Homework 2

Due in class, Friday September 14

1. Suppose we encrypt text with the Hill cipher with key

17	2	3
5	5	5
9	18	2

- What is the decryption key?
- Decrypt the following ciphertext:
  dlxkjufnlbhcuaxqwslsgsmtaticirykkeidayqnpucbsacjunubfqfnttfhmejvvkxfe lutyeihzg-nobbfqqojdnseligrgoqicamzxxgmrgeeoutarydhkisvcvwqtojghxizgptk fuspgfddpvrqukn-jkmywilwvwc

2. Suppose you are given the following plaintext/ciphertext pair that was encrypted with a Hill cipher. Find the key.

Plaintext: itwasthebestoftimesitwastheworstoftimesitwastheageofwisdomitwastheageoffoolishness itwastheepochofbeliefitwastheepochofincredulityitwastheseasonoflightitwastheseasonofda

Ciphertext: epfejaeeqpvrheemummypsjcdbywdcvrheemummypsjcrzaalhyndxsvxbyhxfsjrwdwks nlxljebciqrtyfxfsjmfdphzlkoyozbvfipsjcfxceenjrdsbjvgljvwbvnbzsckfhsooy jjhsfheasgwxxfsjfwlapvmhvgsq

3. Compute the following by performing the Euclidean algorithm by hand (show the successive divisions):

- $\gcd(123, 72)$
- $\gcd(544, 9888)$
- $\gcd(1000, 345)$
- $\gcd(875, 864)$

4. Consider the Euclidean algorithm for computing $\gcd(a, b)$ with remainders $r_1, r_2, \ldots r_k = 0$ at each step.

- Prove that the remainders decrease: that is, $r_j < r_{j-1}$ for all j.
- Prove that r_{k-1} divides both a and b.
- Prove that any common divisor of a and b divides r_{k-1}.
- Using the previous two results, prove that the Euclidean algorithm computes $\gcd(a, b)$.

5. Compute the following multiplicative inverses using the Euclidean algorithm:

- $235^{-1} \mod 999$
- $782^{-1} \mod 1235$