Math 437 – Homework 6

Due 10:15am on Thursday, February 23, 2017

Please indicate any sources you used for a given problem on the solution to that problem. For example, if you worked with another student to get the solution to a problem, please indicate who. You are welcome to work together in small groups, but please try the problems on your own first and write up your own solutions.

Problem 1.

(a) Decrypt the following message that was made with a shift cipher:

HFJXFW ZXJI XMNKY HNUMJWX

(b) Decrypt the following message that was encrypted with a 2×2 Hill cipher

TNHSEQWAYUFTHNCU

if you know that the message starts "HI ALICE"

Problem 2. (Ch. 6 #18) Prove that $a \in \mathbb{Z}_m$ will have a multiplicative inverse in $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

Problem 3. Alice and Bob want to share a secret time to meet up and encrypt it using RSA. Bob chooses $p = 41$ and $q = 59$ and calculates $n = p \cdot q = 2419$ and $m = (p-1)(q-1) = 2320$.

(a) Check that $\gcd(211, m) = 1$ and calculate a find multiplicative inverse for 211 in $\mathbb{Z}_m$.

(b) Bob posts $n = 2419$, $a = 211$ and Alice sends Bob the encrypted time $1187 \pmod{n}$. What is the secret meeting time?