CSC 440
HW3
Ximan Liu

1)

Solve 5x+2 ≡ 3x−7 (mod 31).

2x ≡ -9 (mod 31)
2x ≡ 22 (mod 31)
x ≡ 11

2)

Compute gcd(12345678987654321, 100).

gcd(12345678987654320, 100) = gcd(100, 20) = 20

3)

(1) Compute gcd(4883, 4369).

4883 = 1*4369+514
4369 = 8514+257
514 = 2*257+0.
Therefore, the gcd is 257.

(2) Factor 4883 and 4369 into products of primes.

Both numbers have 257 as a factor. Since then 4883 = 257*19 and 4369 = 257 *17.

4)

Answer exercise 3 in section 6.6 of the textbook. As is usual with the Hill cipher, the letters are encoded from 0 to 25 (a is 0, b is 1, and so forth). Assume that left multiplication was used, as explained in my notes on the Hill cipher. The textbook uses right multiplication which, as I mentioned in lecture, is mathematically fine but uncommon in my experience. Provide the 2x2 encryption matrix as the answer with its values in the range 0 to 25. To make sure you get partial credit in case your matrix is incorrect, show your work as well.
The ciphertext text GEZXDS was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is solved. Find the encryption matrix M.

Suppose the encryption matrix M: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

GEZXDS: 6, 4, 25, 23, 3, 18

SOLVED: 18, 14, 11, 21, 4, 3

$$\begin{bmatrix} 11 & 21 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 25 & 23 \\ 3 & 18 \end{bmatrix}$$

$$\Big\downarrow \text{ inverse mod 26}$$

$$\begin{bmatrix} 3 & 5 \\ 22 & 11 \end{bmatrix}$$

$$\therefore M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 12 & 3 \\ 11 & 2 \end{bmatrix}$$

5)

Answer exercise 12 in section 6.6 of the textbook. One of the methods can be attacked with fewer steps than required by brute force. Indicate which one and describe the attack, clearly explaining why it requires fewer steps than brute force.

Alice and Bob are arguing about which method of multiple encryption they should use. Alice wants to choose keys K1 and K2 and triple encrypt a message m as c=EK1(EK2(EK1(m))). Bob wants to encrypt m as c=EK1(EK1(EK2(EK2(m)))). Which method is more secure? Describe in detail an attack on the weaker encryption method.

Alice's method is more secure. We cannot use meet-in-the-middle attack.
For Bob's method, encrypting twice with permutations is equivalent to encrypting once. Double encryption adds no security. Double encrypting with two different keywords one after another is equivalent to encrypting with a single keyword.
If we use a known plaintext attack and create a list of all possible encryptions of m, then create a list of all possible decryptions of c (plaintext/ciphertext pair m, c), all the task now becomes finding a match between the two lists, EK(EK(m)) for all possible K and DL(DL(c)) for all possible L. (K1, K2) is in matched pairs (L, K). Pair (m, c) can also exclude the pairs matched firstly. In that case, we only need some steps to get the key.