EE2302 Foundations of Information Engineering

Assignment 6 **Due: 6 pm, Oct 19 (Wed)**

Full mark: 14 points

1. (2 points) Find a value of x, where $0 \leq x < 37 \times 87$, that solves the following simultaneous congruences:

$$x \equiv 3 \pmod{37} \text{ and } x \equiv 4 \pmod{87}.$$

2. (3 points) Find a value of x, where $0 \leq x < 7 \times 12 \times 13$, that solves the following simultaneous congruences:

$$x \equiv 5 \pmod{7},\ x \equiv 2 \pmod{12} \text{ and } x \equiv 8 \pmod{13}.$$

3. Consider the use of RSA cipher. The public key of Bob is $N = 55$ and $e = 3$.

   a) (2 points) Alice wants to send the message 16 to Bob. Encrypt the message. Show your steps.

   b) (2 points) Suppose Alice changes her mind and sends another message to Bob. The ciphertext received by Bob is 21. Decrypt the message. Show your steps.

4. Consider the encryption function as follows:

$$E(x) = ax + b \pmod{m}.$$

   If the cipher is used to encrypt messages in English (i.e., an alphabet of 26 letters), then m is chosen as 26.

   a) (1 points) How can we ensure that decryption can be done?
   b) (1 points) What is the value of $\phi(26)$?
   c) (1 points) How many possible keys are there?
   d) (2 points) Suppose $a = 15$, $b = 6$, and the ciphertext (which contains only one single letter) is 21. Find the plaintext.