HOMEWORK 3

1. Solve the following
   a) Given $\gcd(a,b) = 24$, find $\gcd(a,b,16)$.
   b) Given $\gcd(a,b,c) = 12$, find $\gcd(a,b,c,16)$.
   c) Find $\gcd(200,180,450)$.
   d) Find $\gcd(200,180,450,610)$.
2. Using the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t.
   a) 4 and 7
   b) 291 and 42
   c) 84 and 320
   d) 400 and 60
3. Find all solutions to each of the following linear equations:
   a) $3x \equiv 4 (\mathrm{mod} 5)$
   b) $4x \equiv 4 (\mathrm{mod} 6)$
   c) $9x \equiv 12 (\mathrm{mod} 7)$
   d) $256x \equiv 442 (\mathrm{mod} 60)$
4. Encrypt the message "this is an exercise" using one of the following ciphers. Ignore the space between words. Decrypt the message to get the original plaintext.
   a) Additive cipher with key= 20.
   b) Multiplicative cipher with key= 15

c) Affine cipher with key= $(15, 20)$

5. Assume that punctuation marks(periods, question marks, and spaces) are added to the encryption alphabet of a Hill cipher, then a 2×2 key matrix in Z_{29} can be used for encryption and decryption.
   a) Find the total number of possible matrices.
   b) It has been proved that the total number of invertible matrices is $(N^2 - 1)(N^2 - N)$, where N is the number of alphabet size. Find the key domain of a Hill cipher using this alphabet.