Course:	Cryptography
Instructor:	Dr. Odelu Vanga
University:	IIIT Sri City

Practice Problems

1. Evaluate the following:
   (a). 2109 (mod 21)
   (b). $19^{-1} \pmod{1001}$
   (c). $-101 \pmod{1001}$
   (d). Find the x and y such that $1001x + 2001y = d$, where $d = GCD(1001, 2001)$. Show each step to find d as well as x and y.

2. Prove that, $a \pmod m = b \pmod m$ iff $a \equiv b \mod m$. Hint use the definition of congruent modulo, then we have $m|(b-a)$.

3. Use the exhaustive key search to decrypt the following ciphertext, which was encrypted using shift cipher

$$BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD$$

4. Suppose that $k = (5, 21)$ is a key in an Affine Cipher over Z_{31}.
   (a). Express the decryption function $D_k(y)$ in the form of $D_k(y) = ay + b$, where $a, b \in Z_{31}$.
   (b). Prove $D_k(E_k(x)) = x$ for all $x \in Z_{31}$.

5. Prove that the equation $ax = 1 \pmod b$ has unique solution if $GCD(a, b) = 1$.

6. If an encryption function E_k is identical to the decryption function D_k, then the key k is called an *involutory key*.
   (a). Find all the involutory keys in the shift cipher over Z_{26}.
   (b). Suppose that $k = (a, b)$ is a key in an Affine Cipher over Z_n. Prove that k is an involutory key iff $a^{-1} \pmod n = a$ and $b(a+1) \equiv 0 \pmod n$

7. Determine the inverse of the matrices over Z_{29}:

$$\begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

8. An *Affine-Hill Cipher* is the following modification of a *Hill Cipher*: Let m be a positive integer, and define $\mathcal{P} = \mathcal{C} = (Z_{26})^m$. In this cryptosystem, a key k consists of a pair (L, b), where L is an $m \times m$ invertible matrix over Z_{26}, and $b \in (Z_{26})^m$. For $x = (x_1, x_2, \ldots, x_m) \in \mathcal{P}$ and $k = (L, b) \in \mathcal{K}$, we compute $y = E_k(x) = (y_1, y_2, \ldots, y_m)$ by means of the formula $y = xL + b$. Hence, if $L = (l_{i,j})$ and $b = (b_1, b_2, \ldots, b_m)$, then

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m) \begin{pmatrix} l_{1,1} & l_{1,2} & \dots & l_{1,m} \\ l_{2,1} & l_{2,2} & \dots & l_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ l_{m,1} & l_{m,2} & \dots & l_{m,m} \end{pmatrix} + (b_1, b_2, \dots, b_m)$$

Suppose adversary learned that the plaintext

$$adisplayedequation$$

is encrypted to give the ciphertext

$$DSRMSIOPLXLJBZULLM$$

and adversary also knows that $m = 3$. Determine the key, showing all the computations.

9. We describe a special case of a *Permutation Cipher*. Let m, n be positive integers. Write out the plaintext, by rows, in $m \times n$ rectangles. Then form the ciphertext by taking the columns of these rectangles. For example, if $m = 4$, $n = 3$, then we would encrypt the plaintext *cryptography* by forming the following rectangle:

   cryp
   togr
   aphy

   The ciphertext would be *CTAROPYGHPRY*.

   (a). Describe how Bob will decrypt a cyphertext (given values for m and n).

   (b). Decrypt the following ciphertext, which was obtained by using this method of encryption:

   $$MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW$$

10. Test the following cipher generated with *monoalphabetic* or *polyalphabetic* cipher, and find the key length using Kasiski test and confirm using Index of Coincidence

    $$KSMEHZBBLKSMEMPOGAJXSEJCSFLZSY$$

    Then, recover the keyword.