Chapter 2 Homework 2-5, 7, 9-11, 13-18, 24

2. The ciphertext UCR was encrypted using the affine function

$$(9x + 2)(\text{mod } 26)$$

Find the plaintext.

First, we find the numerical values corresponding to UCR.

$U \mapsto 20$
$C \mapsto 2$
$R \mapsto 17$

If $y = 9x + 2(\text{mod } 26)$, then we need to find y^{-1}.

$$\begin{aligned} y^{-1} &\equiv \frac{1}{9}(x - 2)(\text{mod } 26) \\ &\equiv 3(x - 2)(\text{mod } 26) \end{aligned}$$

Now we can decrypt.

$$\begin{aligned} U : y^{-1} &= 3(20 - 2)(\text{mod } 26) \\ &\equiv 54(\text{mod } 26) \\ &\equiv 2(\text{mod } 26) \\ &\mapsto c \end{aligned}$$

$$\begin{aligned} C : y^{-1} &= 3(2 - 2)(\text{mod } 26) \\ &\equiv 0(\text{mod } 26) \\ &\mapsto a \end{aligned}$$

$$\begin{aligned} R : y^{-1} &= 3(17 - 2)(\text{mod } 26) \\ &\equiv 45(\text{mod } 26) \\ &\equiv 19(\text{mod } 26) \\ &\mapsto t \end{aligned}$$

So, the plaintext is cat.

3. Encrypt *howareyou* using the affine function

$$(5x + 7)(\text{mod } 26)$$

What is the decryption function?

First we assign numerical values to the letters.

$$h, o, w, a, r, e, y, o, u \mapsto 7, 14, 22, 0, 17, 4, 24, 14, 20$$

Then, we apply the function to each numerical value.

$$\begin{aligned}
(5 \cdot 7 + 7)(\text{mod } 26) \equiv 42(\text{mod } 26) \equiv 16(\text{mod } 26) &\to Q \\
(5 \cdot 14 + 7)(\text{mod } 26) \equiv 77(\text{mod } 26) \equiv 25(\text{mod } 26) &\to Z \\
(5 \cdot 22 + 7)(\text{mod } 26) \equiv 117(\text{mod } 26) \equiv 13(\text{mod } 26) &\to N \\
(5 \cdot 0 + 7)(\text{mod } 26) \equiv 7(\text{mod } 26) &\to H \\
(5 \cdot 17 + 7)(\text{mod } 26) \equiv 92(\text{mod } 26) \equiv 14(\text{mod } 26) &\to O \\
(5 \cdot 4 + 7)(\text{mod } 26) \equiv 27(\text{mod } 26) \equiv 1(\text{mod } 26) &\to B \\
(5 \cdot 24 + 7)(\text{mod } 26) \equiv 127(\text{mod } 26) \equiv 23(\text{mod } 26) &\to X \\
(5 \cdot 20 + 7)(\text{mod } 26) \equiv 107(\text{mod } 26) \equiv 3(\text{mod } 26) &\to D
\end{aligned}$$

So, *howareyou*$\to$ *QZNHOBXZD*

As for the decryption function ...

$$\begin{aligned}
y &= 5x + 7 \\
x &= 5y + 7 \\
y &= \frac{1}{5}(x - 7)
\end{aligned}$$

So,

$$y^{-1} \equiv \frac{1}{5}(x - 7)(\text{mod } 26)$$

But, we can't have this as we need to find x such that

$$5x \equiv 1(\text{mod } 26)$$

Here, $x = 21$ and we have our decryption function

$$\begin{aligned}
y^{-1} &\equiv 21(x - 7)(\text{mod } 26) \\
&\equiv 21x - 147(\text{mod } 26) \\
&\equiv 21x + 9(\text{mod } 26)
\end{aligned}$$

4. Choose an affine cipher (mod 26). You do a chosen plaintext attach using hahaha. The ciphertext is NONONO. Determine the encryption function.

$$\begin{array}{ll} h \to N & 7 \to 13 \\ a \to O & 0 \to 14 \end{array} \qquad \begin{array}{r} 7\alpha + \beta \equiv 13 (\text{mod } 26) \\ 0\alpha + \beta \equiv 14 (\text{mod } 26) \end{array}$$

$$\begin{aligned} 7\alpha &\equiv -1 (\text{mod } 26) \\ 7\alpha &\equiv 25 (\text{mod } 26) \\ \alpha &= 11 \\ 0(11) + \beta &\equiv 14 (\text{mod } 26) \\ \beta &= 14 \end{aligned}$$

$$\boxed{11x + 14 (\text{mod } 26)}$$

5. The following ciphertext was encrypted by an affine cipher mod 26

CRWWZ

The plaintext starts with ha. Decrypt the message.

$$\begin{array}{ll} h \to C & 7 \to 2 \\ a \to R & 0 \to 17 \end{array} \qquad \begin{array}{r} 7\alpha + \beta \equiv 2 (\text{mod } 26) \\ 0\alpha + \beta \equiv 17 (\text{mod } 26) \end{array}$$

$$\begin{aligned} 7\alpha &\equiv -15 (\text{mod } 26) \\ 7\alpha &\equiv 11 (\text{mod } 26) \\ \alpha &= 9 \\ 0(9) + \beta &\equiv 17 (\text{mod } 26) \\ \beta &= 17 \end{aligned}$$

So, we have

$$9x + 17 (\text{mod } 26)$$

We next need the inverse.

$$\begin{aligned} &\frac{1}{9}(x - 17) (\text{mod } 26) \\ &3(x - 17) (\text{mod } 26) \end{aligned}$$

So,

$$\begin{aligned} W &: 3(22 - 17) (\text{mod } 26) \equiv 15 (\text{mod } 26) \Rightarrow p \\ Z &: 3(25 - 17) (\text{mod } 26) \equiv 24 (\text{mod } 26) \Rightarrow y \end{aligned}$$

Therefore, CRWWZ $\Rightarrow$ happy

7. Suppose we work mod 27 instead of mod 26 for affine ciphers. How many keys are possible? What if we worked mod 29?

We need $(\alpha, 27) = 1$ which excludes all multiples of 3. So, there are 18 choices for α and 27 for β, giving $18(27) = 486$ possible keys.

Since 29 is prime, we have 28 choices for α and 29 for β, giving $28(29) = 812$ possible keys.

9. You want to carry out an affine encryption using the function $\alpha x+\beta$, but you have $\gcd(\alpha, 26) = d > 1$. Show that if $x_1 = x_2 + \left(\frac{26}{d}\right)$, then $\alpha x_1 + \beta \equiv \alpha x_2 + \beta (\text{mod } 26)$. This shows that you will not be able to decrypt uniquely in this case.

Let $(\alpha, 26) = d > 1$, which implies that $d|\alpha$ and $d|26$. Consider $\alpha x_1 + \beta \equiv \alpha x_2 + \beta (\text{mod } 26)$. If we let $x_1 = x_2 + \left(\frac{26}{d}\right)$, then we have

$$\alpha\left(x_2 + \frac{26}{d}\right) \equiv \alpha x_2 (\text{mod } 26)$$

and this gives that

$$\alpha\left(\frac{26}{d}\right) \equiv 0 (\text{mod } 26)$$

Since $d|26$, every choice of α gives 0(mod 26) and thereby will not allow for a unique decryption.

10. Suppose there is a language that on;y has the letters a and b. The frequency of the letter a is .1 and the frequency of b is .9. A message is encrypted using a Vigenere cipher (working mod 2 instead of mod 26). The ciphertext is BABABAAABA.

a) Show that the key length is probably 2.

B A B A B A A A B A
B A B A B A A A B A
Shift of 1 results in 2 coincidences

B A B A B A A A B A
B A B A B A A A B A
Shift of 2 results in 6 coincidences

B A B A B A A A B A
B A B A B A A A B A
Shift of 3 results in 2 coincidences

B A B A B A A A B A
B A B A B A A A B A
Shift of 4 results in 5 coincidences

Any larger shift will result in less than 6 possibilities, so the probable shift is 2.

b) Using the information on the frequencies of the letters, determine the key and decrypt the message.

Since we know the key is 2, we look at every other letter.

Starting with 1

A	B
1	4

B=b, $0 \to a$

Starting with 2

A	B
5	0

A=b, $1 \to b$

So, the key is $(0, 1) \Rightarrow (a, b)$. Therefore, we have

$$\text{BABABAAABA} \Rightarrow \text{bbbbbbbabbb}$$

11. Suppose you have a language with only 3 letters a,b and c, and they occur with frequencies .7, .2, .1, respectively. The following ciphertext message was encrypted by the Vigenere method (shifts are mod 3 instead of mod 26, of course):

    ABCBABBBAC

    Suppose you are told that the key length is 1, 2 or 3. Show that the key length is probably 2, and determine the most probable key.
    To determine the key length, we look at the number of coincidences when we shift 1, 2 or 3 places.

    ```
      A B C B A B B B A C
    A B C B A B B B A C
    ```

    Shift of 1 resulting in 2 occurrences.

    ```
        A B C B A B B B A C
    A B C B A B B B A C
    ```

    Shift of 2 results in 3 occurrences.

    ```
          A B C B A B B B A C
    A B C B A B B B A C
    ```

    Shift of 3 results in 1 occurrence.

    So, the most likely key length is 2.

    Since the key is of length 2, we look at every other letter.

Odds			Starting with 2		
A	B	C	A	B	C
3	1	1	0	4	1
A=a			B=a, $1 = b$		

    So, the probable key is $(0, 1) = (a, b)$.

13. The ciphertext YIFZMA was encrypted by a Hill cipher with the matrix

$$\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$$

    Find the plaintext.

$$K^{-1} = \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix}$$

    and

$$\begin{array}{ccc} Y = 24 & I = 8 & F = 5 \\ Z = 25 & M = 12 & A = 0 \end{array}$$

Then,

$$\begin{bmatrix} 24 & 8 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 56 & -240 \end{bmatrix} = \begin{bmatrix} 4 & 20 \end{bmatrix}$$

This gives *eu* as the start to the plaintext.

$$\begin{bmatrix} 5 & 25 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} -35 & 160 \end{bmatrix} = \begin{bmatrix} 17 & 4 \end{bmatrix}$$

which gives re

and finally

$$\begin{bmatrix} 12 & 0 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 36 & -156 \end{bmatrix} = \begin{bmatrix} 17 & 4 \end{bmatrix}$$

which gives ka.

Take all together, eureka the plaintext.

14. The ciphertext GEZXDS was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is 'solved'. Find the encryption matrix M.

First, $solved \to GEZXDS$ leads us to $18, 14, 11, 21, 4, 3 \to 6, 4, 25, 23, 3, 18$. Then, we have

$$\begin{bmatrix} 18 & 14 \end{bmatrix} K = \begin{bmatrix} 6 & 4 \end{bmatrix}$$
$$\begin{bmatrix} 11 & 21 \end{bmatrix} K = \begin{bmatrix} 25 & 23 \end{bmatrix}$$
$$\begin{bmatrix} 4 & 3 \end{bmatrix} K = \begin{bmatrix} 3 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 11 & 21 \\ 4 & 3 \end{bmatrix} K = \begin{bmatrix} 25 & 23 \\ 3 & 18 \end{bmatrix}$$

This gives

$$\begin{bmatrix} 11 & 21 \\ 4 & 3 \end{bmatrix}^{-1} = \frac{1}{-51} \begin{bmatrix} 3 & -21 \\ -4 & 11 \end{bmatrix} \equiv \begin{bmatrix} 3 & -21 \\ -4 & 11 \end{bmatrix} (\text{mod } 26) \equiv \begin{bmatrix} 3 & 5 \\ 22 & 11 \end{bmatrix} (\text{mod } 26$$

So,

$$K = \begin{bmatrix} 3 & 5 \\ 22 & 11 \end{bmatrix} \begin{bmatrix} 25 & 23 \\ 3 & 18 \end{bmatrix} (\text{mod } 26) \equiv \begin{bmatrix} 90 & 159 \\ 583 & 704 \end{bmatrix} (\text{mod } 26)$$

Finally, we have

$$K = \begin{bmatrix} 12 & 3 \\ 11 & 2 \end{bmatrix}$$

15. Eve captures Bob's Hill cipher machine, which uses a 2-by-2 matrix M mod 26. She tries a chosen plaintext attack. She finds the plaintext *ba* encrypts to *HC* and the plaintext *zz* encrypts to *GT*. What is the matrix M?

$ba \to HC$ $\qquad\qquad$ $zz \to GT$

$1, 0 \to 7, 2$ $\qquad\qquad$ $25, 25 \to 6, 19$

$$\begin{bmatrix} 1 & 0 \\ 25 & 25 \end{bmatrix} M = \begin{bmatrix} 7 & 2 \\ 6 & 19 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 25 & 25 \end{bmatrix}^{-1} = \frac{1}{25} \begin{bmatrix} 25 & 0 \\ -25 & 1 \end{bmatrix}$$

$$\equiv 25 \begin{bmatrix} 25 & 0 \\ -25 & 1 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 1 & 0 \\ 25 & 25 \end{bmatrix}$$

So,

$$M = \begin{bmatrix} 1 & 0 \\ 25 & 25 \end{bmatrix} \begin{bmatrix} 7 & 2 \\ 6 & 27 \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ 13 & 5 \end{bmatrix}$$

16.

(a) The ciphertext text *ENLI* was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is *dont*. Find the encryption matrix.

We have that $dont \to ELNI$, so this gives that $3, 14, 13, 19 \to 4, 11, 13, 8$. Then,

$$\begin{bmatrix} 3 & 14 \\ 13 & 19 \end{bmatrix} K = \begin{bmatrix} 4 & 11 \\ 13 & 8 \end{bmatrix}$$

$$A^{-1} = \frac{1}{-125} \begin{bmatrix} 19 & -14 \\ -13 & 3 \end{bmatrix} \equiv \frac{1}{5} \begin{bmatrix} 19 & -14 \\ -13 & 3 \end{bmatrix} \equiv 21 \begin{bmatrix} 19 & -14 \\ -13 & 3 \end{bmatrix} \pmod{26}$$

When we multiply this out, we get

$$\begin{bmatrix} 399 & -294 \\ -273 & 63 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 9 & 18 \\ 13 & 11 \end{bmatrix}$$

So,

$$K = \begin{bmatrix} 9 & 18 \\ 13 & 11 \end{bmatrix} \begin{bmatrix} 4 & 11 \\ 13 & 8 \end{bmatrix} = \begin{bmatrix} 270 & 243 \\ 195 & 231 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 10 & 9 \\ 13 & 23 \end{bmatrix}$$

(b) Suppose the ciphertext is *ELNK* and the plaintext is still *dont*. Find the encryption matrix. Note that the second column of the matrix is changed, This shows that the entire second column of the encryption matrix is involved in obtaining the last character of the ciphertext.

$$K = \begin{bmatrix} 9 & 18 \\ 13 & 11 \end{bmatrix} \begin{bmatrix} 4 & 11 \\ 13 & 10 \end{bmatrix} = \begin{bmatrix} 270 & 195 \\ 279 & 253 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 10 & 19 \\ 13 & 19 \end{bmatrix}$$

17. Suppose the matrix $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is used for an encryption matrix in a Hill cipher. Find two plaintexts that encrypt to the same ciphertext.

abcd and nopq both encrypt to DELQ.

First, we want to see what any random string will map to. If we try 'abcd', we get

$$\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 11 & 16 \end{bmatrix}$$

and so we get the ciphertext 'DELQ'. We now need to find another plaintext string that maps to 'DELQ'. We can begin with setting up a system of equations, but this time we will take as the ciphertext a translate of those values we obtained from 'abcd'

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 29 & 30 \\ 37 & 42 \end{bmatrix}$$

$$\Rightarrow \begin{cases} w + 3x = 29 \\ 2w + 4z = 30 \\ y + 3z = 37 \\ 2y + 4z = 42 \end{cases}$$

Solving here, we get

$$\begin{cases} w + 3x = 29 \\ 2w + 4x = 30 \end{cases} \Rightarrow (w, x) \to (-13, 14) \equiv (13, 14)$$

and

$$\begin{cases} y + 3z = 37 \\ 2y + 4z = 42 \end{cases} \Rightarrow (y, z) \to (-11, 16) \equiv (15, 16)$$

So, we have that nopq also maps to DELQ.

18. Let a, b, c, d, e, f be integers mod 26. Consider the following combination of the Hill and affine ciphers. Represent a block of plaintext as a pair (x, y) mod 26. The corresponding ciphertext (u, v) is

$$(x, y) \begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} + (e, f) \equiv (u, v) (\text{mod } 26)$$

Describe how you can carry out a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f). You should state explicitly what plaintexts you chose and how to recover the key.

We will need to use three different plaintexts.

- Choose $(x, y) = (0, 0)$.

$$(0, 0) \begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} + (e, f) = (e, f) \equiv (u, v) (\text{mod } 26)$$

- Choose $(x, y) = (1, 0)$.

$$(1,0)\begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} + (e, f) \equiv (a, b) + (e, f) \equiv (u, v) (\text{mod } 26)$$

  We may subtract off (e, f) to find (a, b).

- Choose $(x, y) = (0, 1)$.

$$(0,1)\begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} + (e, f) \equiv (c, d) + (e, f) \equiv (u, v) (\text{mod } 26)$$

  We may subtract off (e,f) to get (c,d).

24. Alice is sending a message to Bob using one of the following cryptosystems. In fact, Alice is bored and her plaintext consists of the letter a repeated a few hundred times. Eve knows what system is being used, but not the key, and intercepts the ciphertext. For systems (a), (b) and (c), state how Eve will recognize that the plaintext is one repeated letter and decide whether or not Eve can deduce the letter and the key.

    (a) Shift cipher
    For a shift cipher, since the input is all one letter, so will the output. So, Eve will be able to tell that the plaintext is all the same letter but will not be able to deduce the key.

    (b) Affine cipher
    With an affine cipher, as with the shift cipher, the same plaintext letter being repeated over and over will map the same ciphertext. There will be no way, however to deduce the key from this ciphertext.

    (c) Hill cipher (with a 2×2 matrix
    Since $a \to 0$, a plaintext of $a \dots a$ will map to all 0's regardless of the choice of K. You cannot tell the original plaintext is from the ciphertext, however, since the choice of K is irrelevant when coding $a \to A$.