CIS 3362 Homework #3: Playfair, Hill, ADFGVX

1) The following ciphertext was encrypted using the Playfair cipher. The first eight letters of the plaintext are "ifyouare". Determine the secret key and decrypt the whole ciphertext. (Note: I may choose to reveal more of the plaintext, but I haven't made that decision yet.)

```
AIVRPFPSPSBFFGNCGAERSPPHREVRPNIWSALCLECLFBWHLUCLUMFGRSHLSDENDCWSD
PDEDPAEDPFADZPODPLCPAWCYSIAYDCLHDBCHSFHFAVABXSKBASXPOHWODWTCGFEPA
QPTCBETLOYGIAEAEBCXBTLPLGPXEUGOGLUEFHLTCVOLCPAPSCQBX
```

The first step is taking the given plaintext encryptions of IF -> AI, YO -> VR, UA -> PF, and RE -> PS. The first two pairs to work with are ideally IF -> AI and UA -> PF. This is because IF and AI share a letter, meaning they must be in a row or column together, and UA -> PF contains A and F, meaning you can form a decent foundation for your Playfair box.

Also note that the initial plaintext is AI VR PF PS PS, and the repetition of the PS means the plaintext actually goes IF YOU ARE RE…, and you can then suppose (from previous trends in plaintexts given in these homeworks) that the next section is READING THIS… Leaps in logic like this can be very useful.

In the Playfair cipher, the keyword goes at the top of course, and from then on, all the letters must be in alphabetical order. Now consider the following possible arrangements of the previously mentioned pair IF -> AI:

F	I	A

I	A			F

These are horizontal because if the arrangements were instead vertical, you would either have A on the third row or you would have F on the very bottom of the table, both of which require long keywords with a lot of unique characters, which is unlikely. Using the intuition that letters after the keyword's letters must be alphabetical, the arrangement `IA--F` is the more auspicious of the two above. This is because B, C, D, E would normally go in that gap, and it's highly possible that this is actually the second row, and two letters among B, C, D, E are contained in the keyword.

Working off this assumption, one can now consider the encryption UA -> PF. Because A and F are already in our tentative arrangement, the letters P and U must be directly above or below A and F respectively. Remembering again the alphabetical nature of this box, the arrangement of P and U below is more likely, since there would again be a gap of two spaces, allowing two letters from the pool Q, R, S, T. Knowing that R, S, and T and fairly common letters, it isn't difficult to imagine a couple of them are in the keyword (just as it's not difficult to imagine Q is *not* in the keyword). And knowing all the letters that come in between F and P, there is probably an "empty" row in between the pair of letters.

Now to show the square all of this supposition leads to (remember that I and J share a box):

I/J	A			F
O	P	Q	R	U
V	W	X	Y	Z

Firstly, where did the last row come from? Well, it's the only thing that makes sense! Those are the last letters of the alphabet after U. Secondly, you'll also notice that the mapping YO -> VR can fill in the empty spaces in the fourth row (as I demonstrated above), and now we know S and T are definitely in the keyword.

From the mapping RE -> PS and the table so far, there is only one arrangement that makes sense:

	E		S	
I/J	A			F
O	P	Q	R	U
V	W	X	Y	Z

Now recall the guess that the plaintext includes READING THIS as the next bit. So AD -> BF, IN -> FG, and GT -> NC. For the first mapping, since AF are arranged like-so in the box above, the only arrangement that makes sense is ABDF. You'll notice that C must also be in the keyword along with T.

For the second and third mappings IN -> FG and GT -> NC, putting G below I/J (right after F) and N below F (leading to NOP…) is practically instinctive. And thus, we now know where the C and T must go, since they must be above G and N respectively.

These conclusions are now compiled into the table:

C	E		S	T
I/J	A	B	D	F
G				N
O	P	Q	R	U
V	W	X	Y	Z

The only letters left are H, K, L, and M, and considering the word *celestial* is part of some of my email addresses, it was fairly easy to guess this was the key—though in general, anyone could probably guess this due to pure intuition or logic.

C	E	L	S	T
I/J	A	B	D	F
G	H	K	M	N
O	P	Q	R	U
V	W	X	Y	Z

Thus, the plaintext is (noting that Q was placed between like letters and also to pad at the end, thus removed from the following text):

IF YOU ARE READING THIS PERHAPS YOU HAVE DETECTED A PATTERN IN MY KEYS THIS YEAR. AS A REWARD, IF YOU ARE THE VERY FIRST, EMAIL ME AND I WILL MAIL YOU A PRIZE VIA THE POSTAL SERVICE. WE WILL SEE HOW LONG IT TAKES TO GET HERE, LOL.

Commentary from Arup: Jade wrote this solution and I had completely forgotten that "celestial" was in her email address!!! My purpose in picking the key word was continuing with the My Little Pony theme from before (my 7 year old is currently obsessed with the ponies, to the point where I actually know several of their names and personality traits.) There is a pony named Princess Celestia!

2) The following was encrypted using the Hill Cipher with a 2 x 2 matrix as the key. Determine both the decryption key as well as the message itself.

```
AUGRRXULTRFUQGBNULYTAGPONPBVPBSUMOFFYVYGLYGTMCOICEESXFPBUHKCYUIDK
RGJEOHDXNHQPBMYBEHYYUNL
```

For this, brute force seemed the easiest solution. Although there are no hints as to the key given (such as a mapping or the like), you can simply traverse through all possible values a, b, c, d for a given encryption matrix. The constraints are that the determinant *ad – bc* must be coprime to 26, so one can simply compose all possible {a, b, c, d} decryption matrices and brute-force decrypt the plaintext for every possible matrix. I created the program **hw3_2.c** to do just that.

If all possibilities are printed, that leads to about 150,000 plaintexts (which is tedious to look through), so I cut it down by 1) printing out only the plaintexts with an IC greater than 0.06, and 2) printing out only the plaintexts containing the substring `THE`. It's not a foolproof method and can be finagled around (for example, checking for only IC > 0.065, or even having the insight to check only for the substring `MESSAGE`), but in any case, the results contain the plaintext:

```
SINCE THE APPROACH HERE IS BRUTE FORCE, I WILL KEEP THIS MESSAGE
SHORT SO YOU HAVE LESS STUFF TO READ THROUGH.
```

which was decrypted using the matrix $\begin{pmatrix} \mathbf{15} & \mathbf{23} \\ \mathbf{7} & \mathbf{16} \end{pmatrix}$.

3) Let M = $\begin{pmatrix} 17 & 11 \\ 7 & 14 \end{pmatrix}$ be the encryption key for the Hill cipher. What is the corresponding decryption key?

There are a couple ways of finding the decryption key.

- Method 1:
    - Find the determinant (again, this is (*ad – bc*)mod26 where M = $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$).
        - (17*14 – 11*7)%26 = 5.
    - Find the inverse of the determinant. This can be from a lookup or EEA:
        - 26 = 5*5 + 1
        - 1 = 26 – 5*5
        - 5^{-1}mod26 = (-5)mod26 = 21.
    - Compose the matrix first as $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$%26
        - {14, -11, -7, 17} = {14, 15, 19, 17}.
    - Multiply the matrix by the inverse of the determinant.
        - {294, 315, 399, 357} = {8, 3, 9, 19}.
    - This is the decryption key: $\begin{pmatrix} \mathbf{8} & \mathbf{3} \\ \mathbf{9} & \mathbf{19} \end{pmatrix}$.
- Method 2:

- Consider the identity $\begin{pmatrix}17 & 11\\ 7 & 14\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} mod 26$. You can compose the following equations in order to find {a, b, c, d}, the decryption key:
  - 17a + 11c = 1mod26
  - 7a + 14c = 0mod26
  - 17b + 11d = 0mod26
  - 7b + 14d = 1mod26
- Use like terms to perform arithmetic with the first and second and third and fourth equations:
  - 7(17a + 11c = 1mod26) -> 119a + 77c = 7mod26
  - 17(7a + 14c = 0mod26) -> 119a + 238c = 0mod26
  - Subtract one from the other: 161c = (-7)mod26 -> 5c = 19mod26
  - Find 5^{-1}mod26:
    - 26 = 5*5 + 1
    - 1 = 26 – 5*5
    - 5^{-1}mod26 = (-5)mod26 = 21
  - Multiply by 21 and mod: **c = 9mod26**
  - Substitute c: 17a + 99 = 1mod26 -> 17a = 6mod26
  - Fine 17^{-1}mod26:
    - 26 = 1*17 + 9
    - 17 = 1*9 + 8
    - 9 = 1*8 + 1
    - 1 = 9 – 1*8 = 9 – 1(17 – 1*9) = -1*17 + 2*9
    - 1 = -1*17 + 2(26-1*17) = 2*26 – 3*17
  - Multiply by 23 and mod: **a = 8mod26**

  - 7(17b + 11d = 0mod26) -> 119b + 77d = 0mod26
  - 17(7b + 14d = 1mod26) -> 119b + 238d = 17mod26
  - Subtract one from the other: 161d = 17mod26 -> 5d = 17mod26
  - Again, 5^{-1}mod26 = 21, so multiply by 21 and mod: **d = 19mod26**
  - Substitute d: 17b + 209 = 0mod26 -> 17b = 25mod26
  - Again, 17^{-1}mod26 = 23, so multiply by 23 and mod: **b = 3mod26**
- Thus, the decryption key is $\begin{pmatrix}\mathbf{8} & \mathbf{3}\\ \mathbf{9} & \mathbf{19}\end{pmatrix}$.

4) You have intercepted a tiny portion of both the plaintext and matching ciphertext of a message encrypted using the Hill cipher with a 2 x 2 matrix key. The plaintext is "BOOK" and the corresponding ciphertext is "ABYE". What are the possible encryption keys based on this information only?

BOOK = [1, 14, 14, 10], ABYE = [0, 1, 24, 4]. The encryption key $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ can be found by setting up a system of equations like so:

- $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1\\ 14\end{pmatrix} = \begin{pmatrix}0\\ 1\end{pmatrix} mod 26$
  - a + 14b = 0mod26

- c + 14d = 1mod26
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 14 \\ 10 \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \end{pmatrix} mod 26$
  - 14a + 10b = 24mod26
  - 14c + 10d = 4mod26
- First, let's find b:
  - You can say: a = (–14b)mod26 = (12b)mod26
  - 14(12b) + 10b = 24mod26
  - 178b = 24mod26
  - 22b = 24mod26 -> 22b = 24 + 26n
  - 11b = 12 + 13n -> 11b = 12mod13
  - To find 11^{-1}mod13:
    - 13 = 1*11 + 2
    - 11 = 5*2 + 1
    - 1 = 11 – 5*2 = 11 – 5(13 – 1*11) = –5*13 + 6*11
    - Thus 11^{-1}mod13 = 6
  - b = 72mod13 = 7mod13
  - b can also be 7+13 = 20
  - **b = 7, 20**
- Now to find a:
  - a + 14b = 0mod26
  - a + 14(7) = 0mod26
  - a = (–98)mod26 = 6mod26
  - **a = 6**
  - Even if you plug in b = 20, you still get a = 6.
- Now to find d:
  - To use a slightly different method, set up the equations:
  - c + 14d = 1mod26 -> 12c + 168d = 12mod26
  - 14c + 10d = 4mod26 -> –12c – 16d = 4mod26
  - Add them together: 152d = 16mod26
  - 22d = 16mod26 -> 22d = 16 + 26n
  - 11d = 8 + 13n -> 11d = 8mod13
  - 11^{-1}mod26 = 6, so: d = 48mod13 = 9
  - d can also be 9+13 = 22
  - **d = 9, 22**
- Now to find c:
  - c + 14d = 1mod26
  - c + 14(9) = 1mod26
  - c = (–125)mod26
  - **c = 5**
  - Even if you plug in d = 22, you still get c = 5.

Thus, these are the possible encryption keys upon this inspection.

$$\begin{pmatrix} 6 & 7 \\ 5 & 9 \end{pmatrix}, \begin{pmatrix} 6 & 7 \\ 5 & 22 \end{pmatrix}, \begin{pmatrix} 6 & 20 \\ 5 & 9 \end{pmatrix}, \begin{pmatrix} 6 & 20 \\ 5 & 22 \end{pmatrix}$$

However, note that {6, 20, 5, 9} and {6, 20, 5, 22} do not have a corresponding inverse (decryption key) since their determinant is 6, which is not coprime with 26. Thus, once we remove these two possibilities, we are down to two possible encryption keys:

$$\begin{pmatrix} 6 & 7 \\ 5 & 9 \end{pmatrix}, \begin{pmatrix} 6 & 7 \\ 5 & 22 \end{pmatrix}$$

5) **By hand**, using the Hill cipher, encrypt the following plaintext, "HAPPYTUESDAY", with the following encryption key: $\begin{pmatrix} 3 & 7 \\ 14 & 19 \end{pmatrix}$.

H	A	P	P	Y	T	U	E	S	D	A	Y
7	0	15	15	24	19	20	4	18	3	0	24

- $\begin{pmatrix} 3 & 7 \\ 14 & 19 \end{pmatrix}\begin{pmatrix} 7 \\ 0 \end{pmatrix} = \begin{pmatrix} 3*7+7*0 \\ 14*7+19*0 \end{pmatrix} = \begin{pmatrix} 21 \\ 98 \end{pmatrix} = \begin{pmatrix} 21 \\ 20 \end{pmatrix} = \begin{pmatrix} V \\ U \end{pmatrix}$
- $\begin{pmatrix} 3 & 7 \\ 14 & 19 \end{pmatrix}\begin{pmatrix} 15 \\ 15 \end{pmatrix} = \begin{pmatrix} 3*15+7*15 \\ 14*15+19*15 \end{pmatrix} = \begin{pmatrix} 150 \\ 495 \end{pmatrix} = \begin{pmatrix} 20 \\ 1 \end{pmatrix} = \begin{pmatrix} U \\ B \end{pmatrix}$
- $\begin{pmatrix} 3 & 7 \\ 14 & 19 \end{pmatrix}\begin{pmatrix} 24 \\ 19 \end{pmatrix} = \begin{pmatrix} 3*24+7*19 \\ 14*24+19*19 \end{pmatrix} = \begin{pmatrix} 205 \\ 697 \end{pmatrix} = \begin{pmatrix} 23 \\ 21 \end{pmatrix} = \begin{pmatrix} X \\ V \end{pmatrix}$
- $\begin{pmatrix} 3 & 7 \\ 14 & 19 \end{pmatrix}\begin{pmatrix} 20 \\ 4 \end{pmatrix} = \begin{pmatrix} 3*20+7*4 \\ 14*20+19*4 \end{pmatrix} = \begin{pmatrix} 88 \\ 356 \end{pmatrix} = \begin{pmatrix} 10 \\ 18 \end{pmatrix} = \begin{pmatrix} K \\ S \end{pmatrix}$
- $\begin{pmatrix} 3 & 7 \\ 14 & 19 \end{pmatrix}\begin{pmatrix} 18 \\ 3 \end{pmatrix} = \begin{pmatrix} 3*18+7*3 \\ 14*18+19*3 \end{pmatrix} = \begin{pmatrix} 75 \\ 309 \end{pmatrix} = \begin{pmatrix} 23 \\ 23 \end{pmatrix} = \begin{pmatrix} X \\ X \end{pmatrix}$
- $\begin{pmatrix} 3 & 7 \\ 14 & 19 \end{pmatrix}\begin{pmatrix} 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 3*0+7*24 \\ 14*0+19*24 \end{pmatrix} = \begin{pmatrix} 168 \\ 456 \end{pmatrix} = \begin{pmatrix} 12 \\ 14 \end{pmatrix} = \begin{pmatrix} M \\ O \end{pmatrix}$

Thus, the ciphertext is **VUUBXVKSXXMO**.

6) The following cipher text was encrypted using the ADFGVX cipher with the 6 x 6 key matrix shown below and the keyword "COMPUTER".

	A	**D**	**F**	**G**	**V**	**X**
A	Q	W	E	R	1	T
D	Y	2	U	I	O	3
F	P	A	4	S	D	5
G	6	F	G	H	7	J
V	K	L	Z	8	X	C
X	V	B	9	N	M	0

AFXFDDXGDFFDGXDGDGVGDDAXVDXD

There are 28 characters. The keyword is 8 letters long. This means that when the ADFGVX-encrypted text was written out in rows, there were 3 full rows of 8 characters 1 row of 4 characters. Now consider the text (which consists of transposed columns) and the keyword (alphabetized). Separate the text out into blocks (and even label them, if you want):

```
AFXF DDX  GDFF DGXD GDGV GDD  AXV  DXD
C    E    M    O    P    R    T    U
```

Place the text below the columns like so (or visualize as such) and then rearrange the columns:

```
C E M O P R T U          C O M P U T E R
A D G D G G A D          A D G G D A D G
F D D G D D X X     ->   F G D D X X D D
X X F X G D V D          X X F G D V X D
F   F D V                F D F V
```

Now with the text arranged properly, you can decrypt using the ADFGVX table with the text reading left to right as (in pairs):

```
AD GG DA DG FG DD XX DD XX FG DV XD FD FV
```

And the plaintext becomes:

```
WHY IS 2020 SO BAD?
```