CIS 3362 Homework #3: Playfair, ADFGVX, Hill, Enigma Solutions

1) (10 pts) By hand, encrypt the plaintext “THISHOMEWORKSALITTLELATE” with the keyword “SPACEROCKS” and the padding character “Q”.

Solution

The omission here was the method of encryption, which was meant to be Playfair. That's my fault. I clarified it for each student who asked. Here is the corresponding Playfair square:

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

Now, let's encrypt each pair:

TH → QI (box)
IS → FC (box)
HO → GK (box)
ME → US (box)
WO → PG (column wrap)
RK → OB (row)
SA → PC (row)
LI → FL (row wrap)
TQ → UT (row + pad)
TL → UJ (box)
EL → DU (column)
AT → CQ (box)
EQ → AU (box)

Final Answer: **QIFCGKUSPGOBPCFLUTUJDUCQAU (Note: In the final answer any I can be substituted by J or vice versa.)**

2) (15 pts) For the Hill cipher, for a language with an **alphabet size of 47,** the encryption key is $\begin{pmatrix}13 & 27\\ 31 & 38\end{pmatrix}$, what is the corresponding decryption key?

Solution

The determinant of the matrix is 13 x 38 – 31 x 27 = 494 – 837 = -343 ≡ 33 (mod 47).

The inverse matrix we desire is $(33^{-1}\, mod\ 47)\begin{pmatrix}38 & -27\\ -31 & 13\end{pmatrix}$. First, determine $33^{-1}\, mod\ 47$.

47 = 1 x 33 + 14
33 = 2 x 14 + 5
14 = 2 x 5 + 4
5 = 1 x 4 + 1

5 – 4 = 1
5 – (14 – 2 x 5) = 1
5 – 14 + 2 x 5 = 1
3 x 5 – 1 x 14 = 1
3(33 – 2 x 14) – 1 x 14 = 1
3 x 33 – 6 x 14 – 1 x 14 = 1
3 x 33 – 7 x 14 = 1
3 x 33 – 7(47 – 33) = 1
3 x 33 – 7 x 47 + 7 x 33 = 1
10 x 33 – 7 x 47 = 1

Taking this equation mod 47, we find that 10 x 33 ≡ 1 (mod 47).
It follows that $33^{-1} \equiv 10\ (mod\ 47)$.

Now, we can find the desired matrix inverse:

$$(10)\begin{pmatrix}38 & -27\\ -31 & 13\end{pmatrix} = \begin{pmatrix}380 & -270\\ -310 & 130\end{pmatrix} \equiv \begin{pmatrix}4 & 12\\ 19 & 36\end{pmatrix}\ (mod\ 47))$$

We can double check the answer (not necessary for full credit) to make sure we didn't make arithmetic errors:

$$\begin{pmatrix}13 & 27\\ 31 & 38\end{pmatrix}\begin{pmatrix}4 & 12\\ 19 & 36\end{pmatrix} = \begin{pmatrix}13 \times 4 + 27 \times 19 & 13 \times 12 + 27 \times 36\\ 31 \times 4 + 38 \times 19 & 31 \times 12 + 38 \times 36\end{pmatrix}$$

$$\equiv \begin{pmatrix}52 - 20 \times 19 & 156 - 27 \times 11\\ 124 - 9 \times 19 & -16 \times 12 + (-9)(-11)\end{pmatrix}$$

$$\equiv \begin{pmatrix}52 - 380 & 156 - 297\\ 124 - 171 & -192 + 99\end{pmatrix} \equiv \begin{pmatrix}-328 & -141\\ -47 & -93\end{pmatrix}$$

$$\equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\ (mod\ 47)$$

3) (15 pts) You've intercepted a message encrypted by the Hill cipher using a 2 x 2 key (alphabet size 26). You also know that the plaintext "CL" maps to the ciphertext "ZD" and that the plaintext "IP" maps to the ciphertext "PH". What are the possible encryption keys? (Note: I didn't show you how to solve this in class, but it represents a type of problem I've put on a quiz. You can solve it via setting up an unknown key, writing down the matrix equations that ensue, followed by solving 2 systems of 2 equations under mod 26.)

Solution

Let the encryption key be $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Using the given information, we get the two following equations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 \\ 11 \end{pmatrix} = \begin{pmatrix} 25 \\ 3 \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 8 \\ 15 \end{pmatrix} = \begin{pmatrix} 15 \\ 7 \end{pmatrix}$$

This allows us to set up a system of 4 equations (2 equations in a and b, 2 equations in c and d) under mod 26:

$$2a + 11b \equiv 25\ (mod26) \qquad 2c + 11d \equiv 3\ (mod26)$$
$$8a + 15b \equiv 15\ (mod26) \qquad 8c + 15d \equiv 7\ (mod26)$$

For both pairs of equations, multiply the top equation by 4:

$$8a + 44b \equiv 100\ (mod26) \qquad 8c + 44d \equiv 12\ (mod26)$$
$$8a + 15b \equiv 15\ (mod26) \qquad 8c + 15d \equiv 7\ (mod26)$$

Then, subtract the bottom equation from the top in each pair and reduce each term mod 26 as necessary:

$$29b \equiv 85\ (mod\ 26) \qquad 29d \equiv 5\ (mod\ 26)$$
$$3b \equiv 7\ (mod\ 26) \qquad 3d \equiv 5\ (mod\ 26)$$

Using the mod inverse chart for mod 26, we find that 3^{-1} mod 26 is 9. Multiply both equations through by 9 and reduce mod 26:

$$27b \equiv 63\ (mod\ 26) \qquad 27d \equiv 45\ (mod\ 26)$$
$$b \equiv 11\ (mod\ 26) \qquad d \equiv 19\ (mod\ 26)$$

Finally, back substitute to find a and c:

$$2a + 11(11) \equiv 25\ (mod26) \qquad 2c + 11(-7) \equiv 3\ (mod26)$$
$$2a \equiv 25 - 121 \equiv -96 \equiv 8\ (mod26) \qquad 2c \equiv 3 + 77 \equiv 80 \equiv 2\ (mod26)$$

Now, rewrite each equation via the definition of mod:

$2a = 8 + 26n$, for some integer n
$a = 4 + 13n$
$a \equiv 4 (mod\ 13)$
This means, that under mod 26, we have:

$a \equiv 4\ (mod\ 26)$ or $a \equiv 17\ (mod\ 26)$

$2c = 2 + 26m$, for some integer m
$c = 1 + 13m$
$c \equiv 1\ (mod\ 13)$
This means, that under mod 26, we have:

$c \equiv 1\ (mod\ 26)$ or $c \equiv 14\ (mod\ 26)$

Thus, we have four possibilities:

$\begin{pmatrix} 4 & 11 \\ 1 & 19 \end{pmatrix}$, $\begin{pmatrix} 4 & 11 \\ 14 & 19 \end{pmatrix}$, $\begin{pmatrix} 17 & 11 \\ 1 & 19 \end{pmatrix}$, or $\begin{pmatrix} 17 & 11 \\ 14 & 19 \end{pmatrix}$.

Finally though, we must make sure that none of these solutions are extraneous. We actually have to plug each of them back into the original two equations to make sure they still work. (All four do still work, so these are the four possible keys based on the given information.)

4) (30 pts) The following ciphertext was encrypted using the Playfair cipher. For the first few days, I won't give any matching plaintext. But, after a few days I'll reveal some characters or the plaintext, and then I'll reveal some more characters again before the due date. Determine the secret key and decrypt the whole ciphertext.

```
rnoprbwdhogmkuohrhnzohdqbfundczdkqsdxipmurknfcdqmeszkdcaftie
qdziksnfkfghkthqopfadcgsabdsfbfrnupahuocnrdgtcrnfcdroqnufvuz
ghupdpfuerrbdypaloghupoecxdsrnmxcaftauidqddsmeszrdfdhqowfcku
ruerhfyrdscxmpkpkpqgqmnvdczdroxreqdeydtwszzifyehxbudrdbvuddh
zdhfudbpdadkersaabzitqrnxrrchqowcr
```

Sample Solution

There aren't too many repeated digrams. Only a few appear 3 or 4 times:

4 times: rn, ds
3 times: sz, dc, ud, er, fc, gh, hq, zd, zi

A reasonable guess is that z is in the bottom right corner of the square, but is interacting with s, d and i, respectively, which are in earlier rows. Of the likely last row letters (V, W, X, Y, and Z), W and Y are the most common, so it stands to reason the S, D, and I are either in the column for W, Y or Z (one of the digraphs could be the result of the column rule.)

This isn't nearly enough to go on, so we must search for more clues.

The next place to look is digraphs that are "flipped". We know for Playfair if we see both "XY" and "YX" in the ciphertext, then the corresponding plaintext is two unique letters in both orders as well. There is only one pair of flipped digraphs that both appear more than once in the ciphertext:

QD and DQ (both appear twice)

The other flipped pairs of note are:

RN and NR (RN appears 4 times, NR once)
DS and SD (DS appears 4 times, SD once)

Q is unlikely to be in the keyword and a pretty good guess is that Q is on row 4. (It's likely that row 5 is pretty close to VWXYZ.) It's likely that D doesn't appear on row 4 so that the box rule is being used for QD and DQ.

Utilizing this list: https://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/digraphs.html we see that the most common flipped digraph is "IT" and "TI". So either QD → "IT" or QD → "TI". The latter seems more likely, if this is the case, then it's likely that T is NOT in the keyword, so we might have something like this:

	D/I?			I/D?
	Q?			T?
V	W	X	Y	Z

The columns for Q and T aren't set and also, if D and I are not in the keyword, D would come before I (to the left), but if both are in the keyword, it's possible that I comes first. (In the latter case, it's more likely both D and I would be on row 1.)

If we use our previous deduction that S, D and I are likely in the columns for W, Y and Z, then either S might be to the left of T (if not in the keyword), or S could be in row 1 or row 2 as part of the keyword. If U is not in the keyword, we get a slightly different picture:

	D/I/S?		I/D/S?	I/D/S?
	D/I/S?		I/D/S?	I/D/S?
	Q	R	T	U
V	W	X	Y	Z

We put R in between Q and T because S is presumably in the keyword in this version.

To get the solution from here without the matching information requires some guessing or further language analysis beyond this. If we use the matching plaintext/ciphertext information given, we have the following pieces of information:

TH → RN (TH encrypts to RN)
IS → OP
KE → RB
YI → WD
SA → HO
BO → GM
UT → KU

The last clue is pretty useful. The only way this can occur is if all three of K, T and U are on the same row or column. Our current guess has them in the same row, so we know have:

	D/I/S?		I/D/S?	I/D/S?
	D/I/S?		I/D/S?	I/D/S?
K	Q	R	T	U
V	W	X	Y	Z

This is very significant, because it insinuates (if our guesses are right), that the following letters are all in the key: L, M, N, O, P. If we put this together with our guess that D, I and S are in the key, we have the following letters in the key:

D, I, S, L, M, N, O, P

Using the pair SA → HO, since S and O are in the keyword, it's likely that A and H are also. This means our keyword uses the following letters:

D, I, S, L, M, N, O, P, H, A

If we use some facts about the instructor, we can see that the word "DOLPHINS" can be formed with these letters. There are some other letters listed above, so it makes sense to add "MIAMI" to the prefix to get the keyword: "MIAMIDOLPHINS" which, when used for the Playfair cipher creates the square:

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

Using this key, we can recover the plaintext:

This key is about as easy as it gets if you know a little bit about me. In fact, I wouldn't be surprised if someone gets this right off the bat just by guessing the key. This message won't have information about any prize but the next one will. Luckily, if you are crafty, you won't have to talk to anyone to claim the homework three prize.

This message has been cleaned up by removing the padding characters ('q') and adding punctuation.

The attached program, playfair.java was used to generate the plaintext above.

5) (30 pts) The following ciphertext was generated using the code found at this link:

```
http://www.cs.ucf.edu/~dmarino/ucf/cis3362/progs/hill.java
```

```
HJLMYYBHFIKQSQEQAKWMSRYRKZPESYBGSCVDBHFBFLDRYKCPBHFQIAXTXDKK
EERJTLYPKOTSBDAMXGBHFACMSVXXNJQIVHHTECOJAADHMGZHTQWWQOWUPXME
CNJESHUUTNGUBDAOFVWQDUQHKOWJSAYFBOIVJBVOBGACFMKNMSERKYGYGRYE
RQAWQOBHFPFWOGAIIIVCQQOXYFICVDBHFGRMYKFIIIVCQOFVMFZYYYKBUMRT
WHXUOOBBEQRYWUOLVFJTQTONUWZDPDBHFXDUGKNWMRNGUBHFOKOCKHSHKSWT
VLZECBFPZLCKHSJCJJASB
```

The encryption key is a 3 x 3 matrix and the hint that will be given (to make decrypting easier) is as follows:

All of the numbers in the 3 by 3 decryption key are taken from the following set: {0, 4, 5, 6, 8, 11, 16, 21, 22, 25}.

Sample Solution

The attached program h3q5.c attempts to generate all 1,000,000 possible matrices based on the description above via brute force. (If you took my CS1 course, it's the same as the odometer program.) If a matrix has a determinant that is divisible by 2 or 13, it can't be the answer, so I skip checking those matrices.

Otherwise, my code scans the whole string for the words "PRIZE" and "THE". (I alluded pretty strongly in class that that message discussed where the prize was hidden, so this is a very reasonable word to look for.) If both words are in the text produced by multiplying the given ciphertext with the generated matrix, my program just prints out the text and matrix.

Somewhat surprisingly, when I ran this on the command line, there were many, many hits. I just started scanning the output in the command prompt window and a little bit after 200,000,000 attempts (just so I could see the status, I printed after a million matrices were generated, which is how I roughly know how many keys I generated before stopping the program), this message popped up:

THIS IS THE MESSAGE YOU WANT TO BREAK. TO FIND THE PRIZE GO TOT HEC'S UNDERGRAD ADVISING OFFICE ON THE SECOND FLOOR OF HEC. GO TO THE MIDDLE ROOM WHERE JENNY HAS HER OFFICE. THERE ARE SEATS. BY THE LEFTMOST ONE, IF YOU ARE FACING THE ROOM, THERE IS A MAGAZINE RACK. FIND THE WIRED MAGAZINE THAT HAS A COVER TITLE, "WELCOME TO MIRROR WORLD." OPEN TO THE PAGE NUMBER OF THE AGE OF YOUR INSTRUCTOR TO FIND THE PRIZE.

The decryption matrix that produced this plaintext was:

$$\begin{pmatrix} \mathbf{5} & \mathbf{0} & \mathbf{8} \\ \mathbf{16} & \mathbf{6} & \mathbf{21} \\ \mathbf{5} & \mathbf{25} & \mathbf{22} \end{pmatrix}$$

As an extra piece of knowledge, the winner of this challenge also got to find out how old I am!!!
(Incidentally, I just turned this age a few days before I planted the prize!)