PMAT 329 Introduction to Cryptography

SOLUTION TO QUESTION 5 OF ASSIGNMENT 1

(5) Suppose you have received the following ciphertext

```
EHAYI HAOOM NSPCM YHYDF OSYUT CWCRV MQEHA YIHEY BMZPS
LZXOS WKIOZ COSEH BHWON KRUNS NNJIV DMQLG BGHRB MSKRJ
EGTCX VOSFC ZCMAM DVXRV IREQV HZZEN MKRHF UPWQQ EHMKI
RBMYM BMZPM JWOYI CWGEX ZKKKS UPRVI OOIFR JWEHX XUYJE
BUHRM KCDTV KKNNS LRAZH CWIRV DCCBA RNCED CPVPF EGTCZ
KJAXV WTBMY MBMZP OBEQL TBHEH XXPFK KMYDP LWOKI SXZNZ
VHWSE YVDEH BHNNQ WHRDE JQHWV DHPBP NZRNN ZDXAB LGZKD
YPCXM POGDW OHOVB BHLWV DNWLR
```

which you know was enciphered with a digraphic Hill cipher. Furthermore, you know that the text begins with the phrase "the only guide." Cryptanalyze the ciphertext. Show your work, and give both the decryption matrix and the resulting plaintext.

Solution. Since a digraphic Hill cipher was used and we know that the ciphertext "EH" corresponds to the plaintext "th," we know that

$$D\begin{pmatrix}E\\H\end{pmatrix} \equiv D\begin{pmatrix}4\\7\end{pmatrix} \equiv \begin{pmatrix}19\\7\end{pmatrix} \equiv \begin{pmatrix}t\\h\end{pmatrix} \pmod{26} \qquad (1)$$

where $D = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ is the decryption matrix. Similarly, we know that

$$D\begin{pmatrix}A\\Y\end{pmatrix} \equiv D\begin{pmatrix}0\\24\end{pmatrix} \equiv \begin{pmatrix}4\\14\end{pmatrix} \equiv \begin{pmatrix}e\\o\end{pmatrix} \pmod{26}\ . \qquad (2)$$

From (1) we obtain

$$\begin{aligned} D\begin{pmatrix}4\\7\end{pmatrix} &\equiv \begin{pmatrix}19\\7\end{pmatrix} \pmod{26} \\ \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}4\\7\end{pmatrix} &\equiv \begin{pmatrix}19\\7\end{pmatrix} \pmod{26}, \end{aligned}$$

and carrying out the matrix multiplication yields

$$\begin{cases} 4a + 7b = 19 \pmod{26} \\ 4c + 7d = 7 \pmod{26} \end{cases} .$$

From (2) we obtain

$$\begin{aligned} D\begin{pmatrix}0\\24\end{pmatrix} &\equiv \begin{pmatrix}4\\14\end{pmatrix} \pmod{26} \\ \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}0\\24\end{pmatrix} &\equiv \begin{pmatrix}4\\14\end{pmatrix} \pmod{26}, \end{aligned}$$

and carrying out the matrix multiplication yields

$$\begin{cases} 0a + 24b \equiv 4 \pmod{26} \\ 0c + 24d \equiv 14 \pmod{26} \end{cases} .$$

From these four equivalences in the variables a, b, c, d we obtain the linear system:

$$\begin{pmatrix} 4 & 7 \\ 0 & 24 \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \equiv \begin{pmatrix} 19 & 7 \\ 4 & 14 \end{pmatrix} \pmod{26} .$$

Unfortunately, we cannot solve this system uniquely modulo 26, since the determinant of the coefficient matrix is 96, and $\gcd(96, 26) \neq 1$ However, we can solve it uniquely modulo 13 since $\gcd(96, 13) = 1$, and lift the solution modulo 13 to a solution modulo 26 using the observation that if $x \equiv a \pmod{13}$, then $x \equiv a \pmod{26}$ or $x \equiv a + 13 \pmod{26}$. The solution of the linear system modulo 13 is:

$$D \equiv \begin{pmatrix} 5 & 11 \\ 1 & 6 \end{pmatrix} \pmod{13} .$$

Attempting to decrypt the ciphertext digraphs corresponding to "the only guide" (using arithmetic modulo 26) yields the plaintext

tUe onYy guidR,

Since the errors are only in the second of the letters in each digraph, we only have to modify the last row of D. Adding 13 to both coefficients in that row yields

$$D \equiv \begin{pmatrix} 5 & 11 \\ 14 & 19 \end{pmatrix} \pmod{26},$$

which yields the correct plaintext. Finally, the decrypted message is

> The only guide to man is his conscience; the only shield to his memory is the rectitude and sincerity of his actions. It is very imprudent to walk through life without this shield, because we are so often mocked by the failure of our hopes and the upsetting of our calculations; but with this shield, however the fates may play, we march always in the ranks of honor.
> – Winston Churchill, Tribute to Neville Chamberlain