Solutions to Math 135 Prelim #2

1. (a) $AB = \begin{bmatrix} -2 & 1 \\ -3 & 2 \end{bmatrix}\begin{bmatrix} -1 & 2 \\ 3 & 3 \end{bmatrix} = \begin{bmatrix} 5 & -1 \\ 9 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 25 \\ 9 & 0 \end{bmatrix} \text{MOD } 26.$

(b) If $C = \begin{bmatrix} 5 & 25 \\ 9 & 0 \end{bmatrix} \text{MOD } 26$, then $\det(C) = -225 = 9 \,\text{MOD } 26$. We find $\det(C)^{-1} = 3 \,\text{MOD } 26$ since $9(3) - 1 \equiv 0 \pmod{26}$, and so

$$C^{-1} = 3\begin{bmatrix} 0 & -25 \\ -9 & 5 \end{bmatrix} = \begin{bmatrix} 0 & -75 \\ -27 & 15 \end{bmatrix} = \begin{bmatrix} 0 & 3 \\ 25 & 15 \end{bmatrix} \text{MOD } 26.$$

2. (a) $\texttt{ELVES} = 4 \times 26^4 + 11 \times 26^3 + 21 \times 26^2 + 4 \times 26 + 18 = 2\ 035\ 558$

(b) $2^7 + 2^6 = 2^4 + 2^3 + 1 = 128 + 64 + 16 + 8 + 1 = 217$

(c) $123 = 64 + 56 + 3 = 1 \times 8^2 + 7 \times 8 + 3 = 173$

(d) $a + b = 1001011$ and $a - b = 100001$

3. (a) Converting both the plaintext and keyword to their numerical equivalents, and adding modulo 26 gives

x	6	0	13	3	0	11	5	19	7	4	6	17	4	24
k	1	8	11	1	14	1	8	11	1	14	1	8	11	1
$y = (x + k) \,\text{MOD } 26$	7	8	24	4	14	12	13	4	8	18	7	25	15	25

and so converting back gives the ciphertext `HIYEOMN EIS HZPZ`.

(b) We begin by finding the numerical equivalents of the ciphertext and the key

plain										
x										
key	X	V	-	X	V	-	X	V	-	X
k	23	21	-	23	21	-	23	21	-	23
cipher	P	K	S	F	I	H	Q	D	N	B
y	15	10	18	5	8	7	16	3	13	1

Since $y = (x + k) \,\text{MOD } 26$ we can subtract modulo 26 to find (part of) the plaintext row, namely

x	18	15	-	8	13	-	19	8	-	4
plain	S	P	-	I	N	-	T	I	-	E

It appears that the plaintext is `SPRING TIME`. This allows us to fill in the missing values in the table and conclude that the numerical equivalent of the last letter of the keyword is 1. Therefore, the keyword is `XVB`.

4. (a) If $A = \begin{bmatrix} 4 & 3 \\ 3 & 1 \end{bmatrix}$, then $\det(A) = -5 = 21 \,\text{MOD}\, 26$. Therefore, $\det(A)^{-1} = 5 \,\text{MOD}\, 26$ since $21(5) - 1 \equiv 0 \pmod{26}$. This gives $A^{-1} = 5 \begin{bmatrix} 1 & -3 \\ -3 & 4 \end{bmatrix} = \begin{bmatrix} 5 & -15 \\ -15 & 20 \end{bmatrix} = \begin{bmatrix} 5 & 11 \\ 11 & 20 \end{bmatrix} \,\text{MOD}\, 26$. The ciphertext matrix corresponding to `ELPF` is $Y = \begin{bmatrix} 4 & 15 \\ 11 & 5 \end{bmatrix}$ and so the plaintext matrix is $A^{-1}Y = \begin{bmatrix} 5 & 11 \\ 11 & 20 \end{bmatrix} \begin{bmatrix} 4 & 15 \\ 11 & 5 \end{bmatrix} = \begin{bmatrix} 11 & 0 \\ 4 & 5 \end{bmatrix} \,\text{MOD}\, 26$. This gives the plaintext as `LEAF`.

(b) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be the unknown key matrix. The plaintext matrix is $X = \begin{bmatrix} 1 & 18 \\ 0 & 4 \end{bmatrix}$ and the ciphertext matrix is $Y = \begin{bmatrix} 1 & 14 \\ 0 & 8 \end{bmatrix}$. Since $AX = Y \,\text{MOD}\, 26$, we find that multiplying the matrices gives us the matrix equation

$$\begin{bmatrix} a & 18a + 4b \\ c & 18c + 4d \end{bmatrix} = \begin{bmatrix} 1 & 14 \\ 0 & 8 \end{bmatrix} \,\text{MOD}\, 26.$$

This gives the system of equations

$$\begin{aligned} a &= 1 \,\text{MOD}\, 26 \\ 18a + 4b &= 14 \,\text{MOD}\, 26 \\ c &= 0 \,\text{MOD}\, 26 \\ 18c + 4d &= 8 \,\text{MOD}\, 26 \end{aligned}$$

Substituting the first equation into the second equation gives $18 + 4b = 14 \,\text{MOD}\, 26$ and so $b = -1 = 25 \,\text{MOD}\, 26$. Substituting the third equation into the fourth equation gives $4d = 8 \,\text{MOD}\, 26$ and so $d = 2 \,\text{MOD}\, 26$. In summary, the key matrix is

$$A = \begin{bmatrix} 1 & 25 \\ 0 & 2 \end{bmatrix}.$$

5. (a) The distance between the string `LBYYS` is $185 = 37 \times 5$ and the distance between the string `RZO` is $160 = 2^5 \times 5$. The distance between the string `WQU` is $190 = 2 \times 19 \times 5$, and the distance between the string `YYF` is $130 = 13 \times 2 \times 5$. There are also several instances of the string `YYS` and even `YY`. The only common factor to all of these distances is 5, and so we conclude from Kasiski's test that the estimated keyword length is 5.

(b) The required probability is

$$\begin{aligned} &\frac{C(6,4) + C(18,4) + C(10,4) + C(5,4) + C(4,4) + C(21,4) + C(17,4) + C(14,4) + C(8,4)}{C(288,4)} \\ &\quad + \frac{C(12,4) + C(6,4) + C(6,4) + C(5,4) + 0 + C(10,4) + C(4,4) + C(6,4) + C(15,4)}{C(288,4)} \\ &\quad\quad + \frac{C(21,4) + C(10,4) + C(14,4) + C(17,4) + C(21,4) + 0 + C(18,4) + C(14,4)}{C(288,4)} \end{aligned}$$

Note that since there are only 3 `N`'s and 3 `X`'s in the ciphertest, it is impossible to select 4 of them.

(c) The required probability is

$$\frac{C(6,2)\cdot C(18,2)}{C(288,4)}+\frac{C(12,3)\cdot C(6,1)}{C(288,4)}.$$

6. Using the initial values and the feedback equation, we can fill in the feedback chart

	b_5	b_4	b_3	b_2	b_1
$t=0$	1	0	0	1	0
$t=1$	1	1	0	0	1
$t=2$	1	1	1	0	0
$t=3$	1	1	1	1	0
$t=4$		1	1	1	1
$t=5$			1	1	1
$t=6$				1	1
$t=7$					1

Note that only the first three values of b_5 are needed in order to determine the first 8 values of b_1. Thus, the keyword is 01001111 and so the Vigenère encipherment is

key	0	1	0	0	1	1	1	1
plain	1	1	1	0	1	1	0	1
cipher	1	0	1	0	0	0	1	0