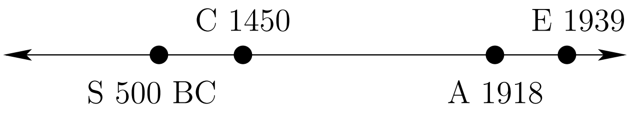
Mathematics 124 Winter 2009 Midterm – Solutions

1. The correct answers are:

Caesar Cipher	monoalphabetic substitution (MA)
Spartan Scytale	transposition (T)
Jefferson's Cipher Wheel	polyalphabetic substitution (PA)

2. A *one-time pad* is an encryption algorithm where the plaintext is combined with a random key or "pad" to produce the ciphertext. The random key is used exactly once. Early implementations of the one-time pad required that both Alice and Bob exchange actual pads containing the keys. If the key is truly random, the same length as the plaintext, never reused, and kept secret, then the one-time pad provides perfect secrecy.

3. (Not drawn to scale)



4. Alberti's cipher wheel is the earliest known cryptographic system to use a polyalphabetic substitution.

5. If $(6x + 2) \equiv (2x + 3) \pmod 9$, then subtracting $2x + 2$ from both sides of the congruence gives $4x \equiv 1 \pmod 9$. Noticing that -2 is a solution to the congruence, we conclude that $x \equiv -2 \pmod 9$ and so $x = 7$ is the smallest positive solution.

6. Since $13 = 1 \times 11 + 2$ we conclude $8 \,\mathrm{DIV}\, 17 = 1$. Since $-13 = -2 \times 11 + 9$ we conclude that $-13 \,\mathrm{DIV}\, 11 = -2$.

7. We find `BEET` $= 1 \times 26^3 + 4 \times 26^2 + 4 \times 26 + 19 = 20\ 403$.

8. We find $11010 + 1001 = 100011$ and $11010 - 1001 = 10001$.

9. Remembering to read the row first then the column from the grid, we conclude that `MATH IS FUN` encodes as

`VV AG XV XF FD XA AA DX XD.`

We now write this across the rows corresponding to `TAG` as follows:

3	1	2
T	A	G
V	V	A
G	X	V
X	F	F
D	X	A
A	A	D
X	X	D

Finally we read down the columns in the order specified by `TAG` to conclude

`VX FX AX AV FA DD VG XD AX`.

10.

(Solution 1) The matrix corresponding to the ciphertext `OMNIVAJI` is

$$Y = \begin{bmatrix} 14 & 13 & 21 & 9 \\ 12 & 8 & 0 & 8 \end{bmatrix}$$

while the matrix corresponding to the plaintext `THE RAVEN` is

$$X = \begin{bmatrix} 19 & 4 & 0 & 4 \\ 7 & 17 & 21 & 13 \end{bmatrix}.$$

If we write the key matrix as

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

then we must have $Y = AX \operatorname{MOD} 26$. Using the first two columns of Y and X implies

$$A \begin{bmatrix} 19 & 4 \\ 7 & 17 \end{bmatrix} = \begin{bmatrix} 14 & 13 \\ 12 & 8 \end{bmatrix} \operatorname{MOD} 26$$

and so

$$A = \begin{bmatrix} 14 & 13 \\ 12 & 8 \end{bmatrix} \begin{bmatrix} 19 & 4 \\ 7 & 17 \end{bmatrix}^{-1} \operatorname{MOD} 26.$$

In order to calculate this inverse, we note that

$$\det \begin{bmatrix} 19 & 4 \\ 7 & 17 \end{bmatrix} = 19 \cdot 17 - 4 \cdot 7 = 295 = 9 \operatorname{MOD} 26.$$

Since $9(3) - 1 = 26$, or equivalently $9(3) \equiv 1 \pmod{26}$, we conclude

$$9^{-1} = 3 \operatorname{MOD} 26$$

so that

$$\begin{bmatrix} 19 & 4 \\ 7 & 17 \end{bmatrix}^{-1} = 3 \begin{bmatrix} 17 & -4 \\ -7 & 19 \end{bmatrix} = \begin{bmatrix} 51 & -12 \\ -21 & 57 \end{bmatrix} = \begin{bmatrix} 25 & 14 \\ 5 & 5 \end{bmatrix} \operatorname{MOD} 26.$$

Finally, we find

$$A = \begin{bmatrix} 14 & 13 \\ 12 & 8 \end{bmatrix} \begin{bmatrix} 25 & 14 \\ 5 & 5 \end{bmatrix} = \begin{bmatrix} 415 & 261 \\ 340 & 208 \end{bmatrix} = \begin{bmatrix} 25 & 1 \\ 2 & 0 \end{bmatrix} \operatorname{MOD} 26.$$

In conclusion, the key matrix is

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

(Solution 2) The matrix corresponding to the ciphertext `OMNIVAJI` is

$$Y = \begin{bmatrix} 14 & 13 & 21 & 9 \\ 12 & 8 & 0 & 8 \end{bmatrix}$$

while the matrix corresponding to the plaintext `THE RAVEN` is

$$X = \begin{bmatrix} 19 & 4 & 0 & 4 \\ 7 & 17 & 21 & 13 \end{bmatrix}.$$

If we write the key matrix as

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

then we must have $Y = AX \operatorname{MOD} 26$. Using the first columns of Y and X implies

$$A \begin{bmatrix} 19 \\ 7 \end{bmatrix} = \begin{bmatrix} 14 \\ 12 \end{bmatrix} \operatorname{MOD} 26$$

and so

$$19a + 7b = 14 \operatorname{MOD} 26 \quad \text{and} \quad 19c + 7d = 12 \operatorname{MOD} 26.$$

Using the third columns of Y and X implies

$$A \begin{bmatrix} 0 \\ 21 \end{bmatrix} = \begin{bmatrix} 21 \\ 0 \end{bmatrix} \operatorname{MOD} 26$$

and so

$$21b = 21 \operatorname{MOD} 26 \quad \text{and} \quad 21d = 0 \operatorname{MOD} 26.$$

Thus we conclude that $b = 1$ and $d = 0$. We now find that $19a + 7 = 14 \operatorname{MOD} 26$ implies

$$19a \equiv 7 \pmod{26}.$$

Noticing that if $a = -1$, then $19a - 7 = -26$ so that

$$a \equiv -1 \equiv 25 \pmod{26}.$$

Finally, $19c = 12 \operatorname{MOD} 26$ can be solved by noticing that if $c = 2$, then $19c - 12 = 26$. In conclusion, the key matrix is

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

11. If x denotes the plaintext numerical equivalent, and $y = E(x)$ denotes the ciphertext numerical equivalent, then in order to determine the plaintext message, we must compute $E^{-1}(y)$. If $y \equiv (7x+2) \pmod{26}$, then $7x \equiv (y-2) \pmod{26}$. Noticing that $7 \times 15 = 105 = 4 \times 26 + 1$, we conclude $7^{-1}\,\mathrm{MOD}\,26 = 15$. This gives $x \equiv 15(y-2) \pmod{26}$ and so $E^{-1}(y) = 15(y-2)\,\mathrm{MOD}\,26$. Therefore,

cipher	C	B	J	C	F	R	W	Y	Y
y	2	1	9	2	5	17	22	24	24
$15(y-2)$	0	-15	105	0	45	225	300	330	330
$15(y-2)\,\mathrm{MOD}\,26$	0	11	1	0	19	17	14	18	18
plain	A	L	B	A	T	R	O	S	S

and so the plaintext is ALBATROSS.

12. There are 81 letters in the ciphertext, and so when the ciphertext is written in $k = 9$ columns (with each column having 9 letters) the plaintext can be read:

TWO ROADS DIVERGED IN A WOOD AND I
TOOK THE ONE LESS TRAVELED BY
AND THAT HAS MADE ALL THE DIFFERENCE

This excerpt is from the poem *The Road Not Taken* by Robert Frost.

Actually, I modified the excerpt slightly in order to make it exactly 81 letters. Frost repeats the word *I* at the start of the second line.

Two roads diverged in a wood, and I—
I took the one less traveled by,
and that has made all the difference.