Solutions to MCS 425 Exercise Set #1 (Spring, 2008)

Sec 2.13, Exercise 2

The encryption function was $y \equiv 9x + 2 \pmod{26}$. So

$$9x \equiv y - 2 \pmod{26}$$
$$x \equiv 9^{-1}(y - 2) \pmod{26}$$
$$x \equiv 3y - 6 \pmod{26}, \quad \text{using } 9^{-1} = 3.$$

Now we decrypt: **U** = 20 $\rightarrow$ $3 \cdot 20 - 6 = 54 \equiv 2$ = **c**
C = 2 $\rightarrow$ $3 \cdot 2 - 6 = 0$ = **a**
R = 17 $\rightarrow$ $3 \cdot 17 - 6 = 45 \equiv 19$ = **t**

The plaintext is **cat**.

Sec 2.13, Exercise 4

Let the encryption function be $E(x) = \alpha x + \beta \pmod{26}$. We know that $E(\mathbf{h}) = \mathbf{n}$ and $E(\mathbf{a}) = \mathbf{o}$, or equivalently, $E(7) = 13$ and $E(0) = 14$.

$$7\alpha + \beta \equiv 13 \pmod{26}$$
$$0\alpha + \beta \equiv 14 \pmod{26}$$

The second equation tells us $\beta \equiv 14$. Substituting this into the first equation gives

$$7\alpha + 14 \equiv 13 \Rightarrow 7\alpha \equiv -1 \pmod{26}.$$

$7^{-1} \equiv 15 \pmod{26}$, so $\alpha \equiv 15(-1) \equiv -15 \equiv 11 \pmod{26}$.

The encryption function is $E(x) = 11x + 14 \pmod{26}$

Sec 2.13, Exercise 8

a) α must be relatively prime to 30; otherwise the mapping $x \rightarrow \alpha x + \beta \pmod{30}$ will not be one-to-one. The choices for α with $0 \le \alpha < 30$ are: 1, 7, 11, 13, 17, 19, 23, 29. There are eight choices for α.

b) **a** and **d** both encrypt to **A**.

a = 0 $\rightarrow$ $10 \cdot 0 + 0 \equiv 0 + 0 \equiv 0 \pmod{30}$, so **a** encrypts to **A**.
d = 3 $\rightarrow$ $10 \cdot 3 + 0 \equiv 30 + 0 \equiv 0 \pmod{30}$, so **d** encrypts to **A**.

In fact, every third character encrypts to **A**.

Sec 2.14, Exercise 1

We are given that the ciphertext **ycvejqwvhqtdtwvwu** was encrypted by a shift cipher. Below are the 26 cyclic shifts of the first three ciphertext character.

0	**ycv**	6	**eib**	11	**jng**	16	**osl**	21	**txq**
1	**zdw**	7	**fjc**	12	**koh**	17	**ptm**	22	**uyr**
2	**aex**	8	**gkd**	13	**lpi**	18	**qun**	23	**vzs**
3	**bfy**	9	**hle**	14	**mqj**	19	**rvo**	24	**wat**
4	**cgz**	10	**imf**	15	**nrk**	20	**swp**	25	**xbu**
5	**dha**								

Which of the 26 shifts above could begin a word? The only possibilities appear (to me) to be **eib**, **imf**, **koh**, **osl**, **qun**, **wat**. For these shifts, we consider two more ciphertext characters (**ej**).

6	**eibkp**	12	**kohqv**	18	**qunwb**
10	**imfot**	16	**osluz**	24	**watch**

Now **watch** appears to be the only alternative. This suggests the decryption key is 24 (**y**), and the encryption key is thus 2 (**c**). Adding 24 to each ciphertext character (or equivalently, subtracting 2), we get the plaintext: **watchoutforbrutus**, or

Watch out for Brutus.

Exercise A

Using R_m with m odd, an uncorrected error in the original message corresponds to $(m+1)/2$ or more errors in the m-bit block transmitted. This occurs with probability

$$\sum_{i=(m+1)/2}^{m} \binom{m}{i} 0.2^i 0.8^{m-i}.$$

Since the expected number of errors is much less than $(m+1)/2$, we obtain a fairly good estimate of the sum by considering only the first term,

$$\binom{m}{(m+1)/2} 0.2^{(m+1)/2} 0.8^{(m-1)/2}.$$

The value of this term for $m = 3, 5, \ldots$ is:

$m = 3$: $3(0.2)^2(0.8) = 0.096$

$m = 5$: $10(0.2)^3(0.8)^2 = 0.0512$

$m = 7$: $35(0.2)^4(0.8)^3 = 0.0287$

$m = 9$: $126(0.2)^5(0.8)^4 = 0.0165$

$m = 11$: $462(0.2)^6(0.8)^5 = 0.0097$

This is less than 0.01, but close enough that including the omitted terms of the sum is likely to bring the sum over 0.01. In fact, the first omitted term is $330(0.2)^7(0.8)^4 = 0.0017$, which does bring the sum over 0.01.

$m = 13$: $1716(0.2)^7(0.8)^6 = 0.0058$

The smallest value of m that works is 13.