Dr. Kanchi
HW 1

1.2 A=5 B=0 C=2 D=3 E=0 F=0 G=5 H=4 I=9 J=2 K=1
L=5 M=0 N=0 O=0 P=5 Q=1 R=1 S=1 T=10 U=1 V=1 W=4 X=7 Y=0 Z=0

xultpaajcxitltlxaarpjhtiwtgxktghidhip
if weallunitewewill causetheriver sto sta
xciwtvgtpilpitghlxiw iwtxgq addS
inthegreatwaterswiththeirblood.

t→e (most frequent) i→t (second most frequent) they are the same distance apart

Is it Caesars cipher? i→t means g→r, h→s maybe?

t→e means w→h .... Yes! This is Caesers cipher!

I think I can fill the rest in now... first changing p→a.

How many letters were identified through a frequency count? t and i ⇒ 2

What is the clear text? If we all unite we will cause the rivers to stain the great waters with their blood. - Tecumseh

1.4.) 1.) 8 letters, 7 bits/letter, 128 chars/letter ⇒ keyspace = 128^8

2.) 8x7 = 56 bits

3.) 8 letters, 5 bits/letter ⇒ 8x5 = 40 bits

4.) a.) 128 bits, 7 bits/letter ⇒ 128/7 = 18.28 so at least 19 letters

b.) 128 bits, 5 bits/letter ⇒ 128/7 = 25.6 so at least 26 letters

1.6 $\frac{1}{5} \bmod 13 = ?$ $5x = 1 \bmod 13$ What times 5 mod 13 = 1?

a.) $40 \bmod 13 = 1$ so $5(8) = 1 \bmod 13$ so $8 = \frac{1}{5} \bmod 13$

Therefore $\frac{1}{5} \bmod 13 = 8$

b.) $\frac{1}{5} \bmod 7 = ?$ $5x = 1 \bmod 7$ What times 5 mod 7 = 1?

5 mod 7 ≠ 1 10 mod 7 ≠ 1 15 mod 7 = 1 ✓

So $5(3) = 1 \bmod 7$ so $3 = \frac{1}{5} \bmod 7$ therefore $\frac{1}{5} \bmod 7 = 3$

c.) $3 \cdot \frac{3}{5} \bmod 7 = ?$ $5x = 6 \bmod 7$ What times 5 mod 7 = 6?

5 mod 7 = 2 10 mod 7 = 3 15 mod 7 = 1 20 mod 7 = 6 ✓

$5(4) = 6 \bmod 7$ therefore $4 = \frac{3 \cdot 2}{5} \bmod 7$ so $3 \cdot \frac{3}{5} \bmod 7 = 4$

1.8 $Z_{11} = \{0, 1 \ldots 9, 10\}$ $(5x) \bmod 11 = 1$

5 mod 11 = 5 10 mod 11 = 10 15 mod 11 = 4 20 mod 11 = 9 25 mod 11 = 3

30 mod 11 = 8 35 mod 11 = 2 40 mod 11 = 7 45 mod 11 = 1

so $5(9) \bmod 11 = 1$ so multiplicative inverse of 5 in Z_{11} is 9.

$Z_{12} = \{0, 1 \ldots 10, 11\}$ $(5x) \bmod 12 = 1$ or $y \bmod 12 = 1$ if $y = 5x$

$y \bmod 12 = 0$ when $y = 0, 12, 24, 36 \ldots$ so $y \bmod 12 = 1$ when $y = 1, 13, 25, 37 \ldots$

When is $y = 1, 13, 25, 37 \ldots$ divisible by 5? when $y = 25$

$5(5) \bmod 12 = 1$ so multiplicative inverse of 5 in Z_{12} is 5

$Z_{13} = \{0, 1 \ldots 11, 12\}$ $(5x) \bmod 13 = 1$ or $y \bmod 13 = 1$ if $y = 5x$

$y \bmod 13 = 1$ when $y = 1, 14, 27, 40, 53 \ldots$ When is y divisible by 5?

When $y = 40$ so $5(8) \bmod 13 = 1$ so multiplicative inverse of 5 in Z_{13} is 8

1.10 a.) Factors of 4: 1, 2, 4 $0 \le n < 4$

$n=0 \Rightarrow$ Factors of n: 0 Is 1 the only common factor of 0 and 4? No

$n=1 \Rightarrow$ Factors of n: 1 Is 1 the only common factor of 1 and 4? Yes

$n=2 \Rightarrow$ Factors of n: 1, 2 Is 1 the only common factor of 2 and 4? No

$n=3 \Rightarrow$ Factors of n: 1, 3 Is 1 the only common factor of 3 and 4? Yes

So $n = 1, 3$ $\varphi(4) = 2$

b.) For remaining problems' steps... see work above

$n = 1, 2, 3, 4$ $\varphi(5) = 4$

c.) $n = 1, 2, 4, 5, 7, 8$ $\varphi(9) = 6$

d.) $n = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$ $\varphi(26) = 12$

1.12 a.) $e_K(x) = y \equiv (ax+b) \bmod 30$

$d_K(y) = x \equiv a^{-1}(y-b) \bmod 30$

b.) $\gcd(a, 30) = 1$ $a = 1, 7, 11, 13, 17, 19, 23, 29$

Key space $= \varphi(30) \times 30 = 8 \times 30 = 240$

c.) $x = \frac{1}{17}(y-1) \bmod 30$ $y = 26, 20, 29, 22, 29$

$y=26$ $\frac{25}{17} \bmod 30 \Rightarrow 17x = 25 \bmod 30$ $x = 5$

$17\{1, 2 \ldots 29, 30\} = \{17, 34, 51, 68, 85, 102, 119, 136, 153, 170, \ldots 493, 510\}$

$y=20$ $\frac{19}{17} \bmod 30 \Rightarrow 17x = 19 \bmod 30$ (1 2 3 4 5 6 7 8 9 10) $x = 17$

$y=29$ $\frac{28}{17} \bmod 30 \Rightarrow 17x = 28 \bmod 30$ $x = 14$

$y=22$ $\frac{21}{17} \bmod 30 \Rightarrow 17x = 21 \bmod 30$ $x = 3$

$x=5$ $x=17$ $x=14$ $x=3$ $x=14$ $\Rightarrow$ frodo

Frodo is from the Shire

1.14 $e_{k_1} = a_1 x + b_1 \quad e_{k_2} = a_2 x + b_2$

a) $e_{k_2}(e_{k_1}(x)) = a_2(a_1 x + b_1) + b_2 = a_2 a_1 x + a_2 b_1 + b_2$

$e_{k_3}(x) = a_2 a_1 x + a_2 b_1 + b_2$ if $a_3 = a_2 a_1$ and $b_3 = a_2 b_1 + b_2$

$d_{k_1}(y) = \frac{1}{a_1}(y - b_1) \quad d_{k_2}(y) = \frac{1}{a_2}(y - b_2) \quad d_{k_3}(y) = \frac{1}{a_3}(y - b_3)$

$e_{k_2}(e_{k_1}(x)) \Rightarrow d_{k_1}(d_{k_2}(y)) = \frac{1}{a_1}\left(\frac{1}{a_2}(y - b_2) - b_1\right) = \frac{1}{a_1}\left(\frac{1}{a_2}y - \frac{b_2}{a_2} - b_1\right)$

$d_{k_3}(y) = \frac{1}{a_3}(y - b_3) = \frac{1}{a_2 a_1}y - \left(\frac{b_2}{a_2} + b_1\right)\frac{1}{a_1}$ if $a_3 = a_2 a_1$,

$-\frac{b_3}{a_3} = -\frac{b_2}{a_2 a_1} - \frac{b_1}{a_1} \Rightarrow \frac{b_3}{a_2 a_1} = \frac{+b_2}{a_2 a_1} + \frac{b_1}{a_1} \Rightarrow b_3 = b_2 + b_1 a_2$

b) If $a_1 = 3, b_1 = 5, a_2 = 11, b_2 = 7$

$a_3 = a_2 a_1 = 33 \overset{\text{mod } 26}{=} 7 \quad b_3 = b_2 + b_1 a_2 = 7 + 55 = 62 \overset{\text{mod } 26}{=} 10$

c) $K = 10 \quad e_{k_2}(e_{k_1}(10)) = e_{k_2}(a_1(10) + b_1 \bmod 26) = e_{k_2}(35 \bmod 26) = e_{k_2}(9)$

$e_{k_2}(9) = a_2(9) + b_2 \bmod 26 = (99 + 7) \bmod 26 = 2 \Rightarrow C$

$e_{k_3}(10) = a_3(10) + b_3 \bmod 26 = (70 + 10) \bmod 26 = 2 \Rightarrow C$

d) No, the keyspace is not increased, because we just proved that every double encrypted affine cipher can be written as a single encrypted affine cipher. Therefore, there is not any extra benefit to doubly encrypting an affine cipher, and no extra keyspace.