HW2 SOLUTION

1) Using a shift cipher to encrypt a 1 letter message is similar to using a one time pad - any plaintext could encrypt to any ciphertext and there is not enough information revealed from the ciphertext to allow further analysis (ie: frequency analysis). In this case,

$H(P) = H(P|C) \Rightarrow$ perfect secrecy is maintained

Let's suppose all 26 english letters are equal in frequency

$$H(P) = -\underset{\substack{\uparrow \\ \text{26 total letters}}}{26}\left(\frac{1}{26}\underset{\substack{\uparrow \\ p(x)=\frac{1}{26} \text{ for ea. letter}}}{\log_2 \frac{1}{26}}\right)$$

$$H(P) = -\log_2 \frac{1}{26}$$

$$H(P|C) = -\sum p(C) \sum p(P|C) \log_2 p(P|C)$$

$$P(C) = \underset{\substack{\uparrow \\ p(PT='a')}}{\left(\frac{1}{26}\right)}\underset{\substack{\uparrow \\ p(K \text{ that encrypts 'a'})}}{\left(\frac{1}{26}\right)} + \underbrace{\left(\frac{1}{26}\right)\left(\frac{1}{26}\right)}_{\text{repeated for ea. of the 26 plaintext}} + \ldots$$

$$= \cancel{26}\left(\frac{1}{26}\right)\left(\frac{1}{26}\right) = \frac{1}{26}$$

$$P(P|C) = \frac{P(P,C)}{P(C)} = \frac{P(P)P(K)}{P(C)} = \frac{\left(\frac{1}{26}\right)\left(\frac{1}{26}\right)}{\frac{1}{26}} = \underset{\substack{\uparrow \\ \text{for each combo of } P|C}}{\frac{1}{26}}$$

$$H(P|C) = -\underset{\substack{\uparrow \\ \text{repeated for all cipher letters}}}{26}\left[\underset{\substack{\uparrow \\ p(C) \text{ for ea. letter}}}{\frac{1}{26}}\left(\underset{\substack{\uparrow \\ \text{26 letter combos}}}{26}\left(\frac{1}{26}\underset{\substack{\uparrow \\ p(P|C)}}{\log_2 \frac{1}{26}}\right)\right)\right]$$

$$H(P|C) = -\log_2 \frac{1}{26}$$

$$\therefore\ H(P) = H(P|C)$$

2)

	a	b	c
K_1	C	A	B
K_2	A	B	C
K_3	B	C	A

$p(a) = 0.8$ $\quad$ $p(K_1) = \frac{1}{3}$

$p(b) = 0.15$ $\quad$ $p(K_2) = \frac{1}{3}$

$p(c) = 0.05$ $\quad$ $p(K_3) = \frac{1}{3}$

a) $$H(P) = -\sum_{x \in P} p(x) \log_2 p(x)$$

$$= -\left[p(a)\log_2 p(a) + p(b)\log_2 p(b) + p(c)\log_2 p(c) \right]$$

$$= -\left[0.8 \log_2 0.8 + 0.15 \log_2 0.15 + 0.05 \log_2 0.05 \right]$$

$$\boxed{= 0.884}$$

b) see next page

b) $H(P|C) = -\sum p(C) \sum p(P|C) \log_2 p(P|C)$

* determine the necessary components:
p(C) for ea. ciphertext value:

$p(A) = p(b)p(K_1) + p(a)p(K_2) + p(c)p(K_3)$
$= 0.333$ (or $\frac{1}{3}$)

$p(B) = p(c)p(K_1) + p(b)p(K_2) + p(a)p(K_3)$
$= 0.333$ (or $\frac{1}{3}$)

$p(C) = p(a)p(K_1) + p(c)p(K_2) + p(b)p(K_3)$
$= 0.333$ (or $\frac{1}{3}$)

p(P|C) for ea. PT and CT combo:

$p(a|A) = \frac{p(a)p(K_2)}{p(A)} = \frac{(0.8)(\frac{1}{3})}{(\frac{1}{3})} = 0.8$
$p(b|A) = 0.15$
$p(c|A) = 0.05$

$\left.\begin{array}{l} p(a|B) = 0.8 \\ p(b|B) = 0.15 \\ p(c|B) = 0.05 \end{array}\right\}$ same as above

$\left.\begin{array}{l} p(a|C) = 0.8 \\ p(b|C) = 0.15 \\ p(c|C) = 0.05 \end{array}\right\}$ same as above

$H(P|C) = -\left[\left(\frac{1}{3}\right)\left(.8\log_2 .8 + .15\log_2 .15 + .05\log_2 .05\right) + \ldots\right]$
$= -\left[3\left(\frac{1}{3}\right)\left(.8\log_2 .8 + .15\log_2 .15 + .05\log_2 .05\right)\right]$
$\boxed{= .884}$

c) No information about the plaintext is revealed by the ciphertext because $H(P) = H(P|C)$. If, however $E_{K_3}(a) = C$ and $E_{K_3}(b) = B$, this would not be the case. In that scenario $H(P|C) < H(P)$ because it is more likely that B decrypts to b than any other plaintext.

3) problem #1a pg 107

$101 = 5 \cdot 17 + 16$

$17 = 16 \cdot 1 + 1 \leftarrow \gcd(17, 101) = 1$ ✓

$1 = 17 \cdot 1 - 16 \cdot 1$ 1 as linear combination of 16, 17

$16 = 101 \cdot 1 + 17(-5)$ substitute...

$1 = 17 \cdot 1 - (101 \cdot 1 + 17(-5))$

$= 17 \cdot 6 + 101(-1)$ $\boxed{x = 6 \quad y = -1}$

4) $101 = (6)15 + 11$

$15 = (1)11 + 4$

$11 = (2)4 + 3$

$4 = (1)3 + \boxed{1}$ $\gcd(101, 15) = 1$ therefore $15^{-1} \pmod{101}$ does in fact exist!

$3 = (3)1 + 0$

$$
\begin{aligned}
1 &= 4 - (1)3 \\
&= 4 - (1)(11 - (2)4) \\
&= 4 - (1)11 + (2)4 \\
&= (3)4 - (1)11 \\
&= (3)(15 - (1)11) - (1)11 \\
&= (3)15 - (3)11 - (1)11 \\
&= (3)15 - (4)11 \\
&= (3)15 - (4)(101 - (6)15) \\
&= (3)15 - (4)101 + (24)15 \\
&= (27)15 - (4)101
\end{aligned}
$$

$\boxed{15^{-1} \pmod{101} \equiv 27}$

$\boxed{101^{-1} \pmod{15} \equiv -4 \equiv 11 \pmod{15}}$

5) prob #4 pg 104

30030 mod 257 = 218
257 mod 218 = 39
218 mod 39 = 23
39 mod 23 = 16
23 mod 16 = 7
16 mod 7 = 2
7 mod 2 = $\boxed{1}$

Just use Euclidean Algorithm (not extended), since all you need is gcd.

$\boxed{\gcd(257, 30030) = 1}$

6) $901^{-1} \pmod{2968}$

$2968 = (3)901 + 265$
$901 = (3)265 + 106$
$265 = (2)106 + \boxed{53}$
$106 = (2)53) + 0$

gcd(901, 2968) = 53 :(

$\boxed{\text{No inverse exists!}}$

7) a) $12x \equiv 28 \pmod{42}$ gcd(a, r, n) = 2, so reduce eqn

$6x \equiv 14 \pmod{21}$ gcd(a, n) = 3 therefore:
1) cycle repeats $\frac{21}{3} = 7$
2) all r should be multiple of 3

$3 \nmid 14$ therefore

$\boxed{\text{No solution}}$

⑥

b) $12x \equiv 30 \pmod{42}$ $\gcd(c, r, n) = 6$ so reduce (expect 6 answers)

$2x \equiv 5 \pmod{7}$ $\gcd(c, n) = 1$

1) cycle repeats every $n = 7$

2) all values of r are possible

$2^{-1} \pmod{7} = 11$ because $2 \cdot 11 = 22$ and $3 \cdot 7 = 21$.

$2^{-1} \cdot 2x \equiv 5 \cdot 2^{-1} \pmod{7}$

$x \equiv 55 \pmod{7}$

$x \equiv 6 \pmod{7}$

$$\boxed{x \equiv \{6, 13, 20, 27, 34, 41\}}$$

8 a) $x^2 \underset{31}{\equiv} 10$ 31 is prime, $31 \underset{4}{\equiv} 3$

check $x \underset{31}{\equiv} \pm 10^{(31+1)/4}$ $x \underset{31}{\equiv} \pm 10^8 = \{14, 17\}$ try these

$14^2 \underset{31}{\equiv} 10$ ✓ so $\boxed{x = \{14, 17\}}$

b) $x^2 \underset{24}{\equiv} 9$ 24 composite, split into $3 \cdot 8$

$x^2 \underset{3}{\equiv} 0$ (1 soln) $x^2 \underset{8}{\equiv} 1$ $x = \{1, 3, 5, 7\}$ (4 solns)

$x \underset{3}{\equiv} 0$	$x \underset{3}{\equiv} 0$	$x \underset{3}{\equiv} 0$	$x \underset{3}{\equiv} 0$
$x \underset{8}{\equiv} 1$	$x \underset{8}{\equiv} 3$	$x \underset{8}{\equiv} 5$	$x \underset{8}{\equiv} 7$
$\boxed{x=9}$	$\boxed{x=3}$	$\boxed{x=21}$	$\boxed{x=15}$

find with trial & error or spreadsheet or Gauss

$x = \{3, 9, 15, 21\}$

c) $x^2 \underset{17}{\equiv} 5$ 17 prime, $a \neq 1$, $17 \underset{4}{\not\equiv} 3$ trial & error or Excel

$\boxed{\text{no solution}}$