PROBLEM 1. (a) Since the text is in the English language, the encoded symbol F corresponds to either A or I (these are the only one letter words in English). So we can check both the cases wether F is the mapping of I or the mapping of A. In the first case, $k = -3$ and if we break the ciphertext based on $k = -3$ the plaintext is meaningless. But if F stands for A then $k = 5$ and based on it, the plaintext is : PROPERTY IS A NUISANCE.

(b) We try to assign maximum frequecy symbol to the letter E and then use the knowledge of the English language to see if the assignment makes sense. For the second example if we map symbol G (which is the most frequent symbol in the encoded string) to the letter E, then we get that $k = 2$ which gives us the plaintext, "WEAKNESS OF ATITUDE BECOMES WEAKNESS OF CHARACTER".

PROBLEM 2. (a) Since the plaintext letter "O" is mapped to two different symbols, the cipher is polyalphabetic.

(b) Assuming it was a Vignere cipher the key used was SIGNAL. Use the table on page 117 of the notes to find the key.

PROBLEM 3. The plaintext is "IF WE HAVE NO PEACE IT IS BECAUSE WE HAVE FORGOTTEN THAT WE BELONG TO EACH OTHER". Since the length of the key is 8 letters, we divide the symbols of the encoded string into the 8 groups EIUEEBER, INTSFNEA, VEAVTEOE, HAEHOTGT, EEBEGANO, WPSWRHOH, ACCATWTH, FOIEOTIC. We then write them down as a column of letters below each letter of the key in alphabetical order: the first group INTSFNEA is written below the letter C of the key; FOIEOTIC is written below U and so on. We then read off row-wise to find the plaintext.

PROBLEM 4. (a) Let $d_1 = \gcd(a, b)$ and let $d_2 = \gcd(a, b + ca)$ for some $c \in \mathbb{Z}$. Clearly $d_2 \geq d_1$ because d_1 divides both a, b thus it also divides $a, b+ca$. Assume that $d_2 > d_1$. Clearly we have

$$\begin{aligned} a &= d_1 k_1 \\ b &= d_1 m_1 \\ a &= d_2 k_2 \\ b + ca &= d_2 m_2 \end{aligned}$$

for some integers k_1, k_2, m_1, m_2. From the last equation we see that

$$\frac{b}{d_2} + \frac{ca}{d_2} = m_2$$

Also the third equation tells us that $\frac{ca}{d_2}$ is an integer. Thus $m_2 - \frac{ca}{d_2}$ is also an integer which implies that $\frac{b}{d_2}$ is an integer. Thus d_2 divides a, b. But $d_2 > d_1$ contradicts the fact that d_1 is the gcd of a, b. Thus $d_2 = d_1$.

(b) From the first part we have

$$\gcd(a, b) = \gcd(a, b + 2a) = \gcd(a + 2(b + 2a), b + 2a) = \gcd(2b + 5a, b + 2a)$$

(c) Let $d_1 = \gcd(ma, mb)$ and $d = \gcd(a, b)$. Note that we only need to consider $m \geq 2$. We first show that d_1 is a multiple of m. Clearly we have

$$\begin{aligned} ma &= d_1 k_1 \\ mb &= d_1 n_1 \\ a &= dk_2 \\ b &= dn_2 \end{aligned}$$

for some integers k_1, n_1, k_2, n_2. Suppose $d_1 = ml + r$ for some l and $0 < r < m$. Then we have that

$$a = (l + \frac{r}{m})k_1$$

from the first equation. Since m does not divide r, it must divide k_1. Similarly m must divide n_1. Thus we have

$$\begin{aligned} ma &= d_1 m k_1' \\ mb &= d_1 m n_1' \end{aligned}$$

for some integers k_1', n_1'. Which implies that

$$\begin{aligned} a &= d_1 k_1' \\ b &= d_1 n_1' \end{aligned}$$

which implies that d_1 must be equal to d (since $d = \gcd(a, b)$) which is a contradiction, since md clearly divides both ma, mb thus $d_1 \geq md > d$ (since $m \geq 2$). This implies that r must be zero which means that $d_1 = ml$. As a result we have

$$\begin{aligned} ma &= mlk_1 \\ mb &= mln_1 \end{aligned}$$

Clearly $l \geq d$ and we cannot have $l > d$ as this would contradict the fact that $d = \gcd(a, b)$. Thus $l = d$.

(d) Since p is a prime the only factors of p are 1 and p, the only possiblities for the common factor between p and a are either 1 or p.

PROBLEM 5. 1. Using Euclid's algorithm we see that the gcd is 12.

2. Using extended Euclid's algorithm we see that $144 \cdot (-2) + 60 \cdot (5) = 12$. Thus $\alpha = 5, \beta = -2$.