Question 1:
Definition of Vigenere Poly-Alphabetic Cipher Construction.
This cipher does not allow corresponding characters in the plaintext and ciphertext to be the same. This would mean $c = m + k,\ k \neq 0$, as that would result in $c = m$.
Fix l as the message length where $l > 0$. Fix i as the current position within the plaintext, key or ciphertext
Fix the alphabets {A, B, …, Z} corresponding to integers {0, 1, …, 25}
Gen: Choose a key from $K = \{ 1, ..., 25 \}^t$ of message length t where $t > 0$, according to uniform distribution
Enc: Given a key $k \in \{1, ..., 25\}^t$ and a message $m \in \{0, 1, ..., 25\}^l$, the encryption algorithm will produce a ciphertext $c := (k_{i \, mod \, t} + m_i) \, mod \, 26$
Dec: Given a key $k \in \{1, ..., 25\}^t$ and a ciphertext $c \in \{0, 1, ..., 25\}^l$, the decryption algorithm will produce the message $m := (c_i - k_{i \, mod \, t}) \, mod \, 26$

Correctness of the construction would mean that $Dec_k(Enc_k(m)) = m$ where m is the plaintext message to be encrypted.

Question 2:
Correctness of the cipher would be $Dec_k(Enc_k(m)) = m$
$Dec_k((k_{i \, mod \, t} + m_i) mod \, 26) = ((k_{i \, mod \, t} + m_i) \, mod \, 26 - k_{i \, mod \, t}) \, mod \, 26 = m_i$ (modulo subtraction)

Question 3:
Define a game where the adversary chooses to send 2 messages, m_0 and m_1 to a system which will randomly encrypt either of the message m_b, using the above vigenere cipher, and show the adversary back the ciphertext of the selected message c_b. Where b is either 0 or 1 corresponding to either message 0 or message 1 was sent.

The adversary can choose to let the message contain only a single letter, and for both the messages, choose different letters to send. For example, $m_0 = \{B\}^l$ and $m_1 = \{C\}^l$, where l is an arbitrary length of the message to be sent. When sent to the system, if the ciphertext received back, c_b contains the letter B, this would mean that m_1 was selected since the letter B would not appear in the ciphertext if m_0 was encrypted. This would be the same if the letter C would be to appear, indicating that m_0 was encrypted instead.
Thus the adversary is able to predict which message was chosen for encryption and hence win the game with a probability higher than 0.5, indicating that this is higher than just random chance.

Question 4:

$Pr[C = 5] = \frac{6}{36} = \frac{1}{6}$ (X=0 & K=5, X=5 & K=0, X=1 & K=4, X=4 & K=1, X=2 & K=3, X=3& K=2)

$Pr[X = x] = Pr[K = k] = \frac{1}{6}$ (values are chosen uniformly and independently)

1. $Pr[X = 1, K = 2 \mid C = 5]$
   $= \frac{Pr[X=1, K=2] \cap Pr[C=5]}{Pr[C=5]} = 0$ (knowing C = 5, X=1 and K=2 will result in C = 1+2 = 3 therefore not possible)
   $Pr[X = 1 \mid C = 5, K = 2]$
   $= \frac{Pr[X=1] \cap Pr[C=5, K=2]}{Pr[C=5, K=2]} = 0$ (knowing C=5 and K=2, X cannot be 1 therefore not possible)

2. $Pr[K = 3 \mid X = 2]$
   $= \frac{Pr[K=3, X=2]}{Pr[X=2]}$ (Conditional Probability)
   $= \frac{\frac{1}{36}}{\frac{6}{36}} = \frac{1}{6}$ (Joint Probability)

3. $Pr[X = 0] = Pr[X = 1] = Pr[X = 2] = Pr[X = 3] = Pr[X = 4] = Pr[X = 5] = \frac{1}{6}$
   $Pr[X = 0 \mid C = 5]$
   $= \frac{Pr[X=0, C=5]}{Pr[C=5]}$ (Conditional Probability)
   $= \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$
   $Pr[X = 1 \mid C = 5] = \frac{Pr[X=1, C=5]}{Pr[C=5]} = \frac{1}{6}$ (same as above)
   $Pr[X = 2 \mid C = 5] = \frac{Pr[X=2, C=5]}{Pr[C=5]} = \frac{1}{6}$ (same as above)
   $Pr[X = 3 \mid C = 5] = \frac{Pr[X=3, C=5]}{Pr[C=5]} = \frac{1}{6}$ (same as above)
   $Pr[X = 4 \mid C = 5] = \frac{Pr[X=4, C=5]}{Pr[C=5]} = \frac{1}{6}$ (same as above)
   $Pr[X = 5 \mid C = 5] = \frac{Pr[X=5, C=5]}{Pr[C=5]} = \frac{1}{6}$ (same as above)

4. $Pr[C = 1] = \frac{2}{36} = \frac{1}{18}$ (X=0 & K=1, X=1 & K=0)
   $Pr[X = 0 \mid C = 1]$
   $= \frac{Pr[X=0, C=1]}{Pr[C=1]}$ (Conditional Probability)
   $= \frac{\frac{1}{36}}{\frac{1}{18}} = \frac{1}{2}$
   $Pr[X = 1 \mid C = 1] = \frac{Pr[X=1, C=1]}{Pr[C=1]} = \frac{1}{2}$ (same as above)
   $Pr[X = 2 \mid C = 1] = \frac{Pr[X=2, C=1]}{Pr[C=1]} = 0$ ($Pr[X = 2 \cap C = 1]$ does not exist)
   $Pr[X = 3 \mid C = 1] = \frac{Pr[X=3, C=1]}{Pr[C=1]} = 0$ ($Pr[X = 3 \cap C = 1]$ does not exist)
   $Pr[X = 4 \mid C = 1] = \frac{Pr[X=4, C=1]}{Pr[C=1]} = 0$ ($Pr[X = 4 \cap C = 1]$ does not exist)
   $Pr[X = 5 \mid C = 1] = \frac{Pr[X=5, C=1]}{Pr[C=1]} = 0$ ($Pr[X = 5 \cap C = 1]$ does not exist)

Question 5:
$Pr[M = m \mid C = c] = Pr[M = m' \mid C = c]$
Assuming that the scheme is perfectly secret
LHS: $Pr[M = m \mid C = c] = Pr[M = m]$ (Definition 2.3)
RHS: $Pr[M = m' \mid C = c] = Pr[M = m']$ (Definition 2.3)
so $Pr[M = m] = Pr[M = m']$

This will not hold true for every distribution on the message space M. Only a message space with a uniform distribution would be able to prove $Pr[M = m \mid C = c] = Pr[M = m' \mid C = c]$ as every message is equally likely to be chosen. However, any non-uniform message space would refute this as the probability of choosing m would be different from the probability of choosing m'.