1. Consider the shift cipher, and the distribution Pr[M = 'one'] = ½, Pr[M = 'ten'] = ½

What is the probability that C='rqh'?

> The only way this ciphertext can occur is if $M = one$ and $K = 3$
>
> Hence, the probability $Pr[C = rqh] = Pr[M = one] * Pr[K = 3] = 1/2 * 1/26 = 1/52$

2. Define a version of the Vigen'ere cipher with an n-letter key working only on ciphertexts of n letters. Show that this cipher is perfectly secret.

> The Vigen'ere cipher we define here requires the message to be n-letter, so ciphertext is also n-letter. For each letter in the message, there are 26 choices with equal possibility $1/26$. When it comes to n-letter, there will have 26^n different message. For n-letter key, we require each letter occurs with the possibility $1/26$. Then we can conclude this version of the Vigen'ere cipher is perfectly secret.
>
> Here is the proof:
>
> **What we assume**: assume a_i is any letter from the set A with 26 letters, $a_i \in A, a_i, 1 \leq i \leq 26$. For every message $m = m_1 \cdots m_n, m \in M$, we have $Pr[m_k = a_i] = 1/26, 1 \leq k \leq n, Pr[M = m] = 1/26^n$, and for every key $k = k_1 \cdots k_n, k \in K$, we have $Pr[k_z = a_i] = 1/26, 1 \leq z \leq n$.
>
> **Proof:**
>
> For every character m_i, it could be a letter $a_i, 0 \leq i < 26$ with equal probability $1/26$. As the k_i can be a letter a_j with equal probability $1/26$ as well, so the encrypted character c_i can be
>
> When $m_1 = a_{26}, k_1 = a_2$, then the encrypted character $c_1 = a_1$, the probability is $Pr[m_1 = a_{26} \wedge k_1 = a_2] = Pr[m_1 = a_{26}] * Pr[k_1 = a_2] = 1/26^2$
>
> When $m_1 = a_{25}, k_1 = a_3$, then the encrypted character $c_1 = a_1$, the probability is $Pr[m_1 = a_{25} \wedge k_1 = a_3] = Pr[m_1 = a_{25}] * Pr[k_1 = a_3] = 1/26^2$
>
> $\ldots$
>
> When $m_1 = a_1, k_1 = a_1$, then the encrypted character $c_1 = a_1$, the probability is $Pr[m_1 = a_1 \wedge k_1 = a_1] = Pr[m_1 = a_1] * Pr[k_1 = a_1] = 1/26^2$
>
> Here we can see, when $c_1 = a_1$, there are 26 distinct pair (m_1, k_1) to get that, so $Pr[c = a_1 | m_1 = a_i] = Pr[k_1 = a_j] = 1/26$
>
> We have $Pr[m_1 = a_i | c_1 = a_1] = \frac{Pr[c=a_1]|m_1=a_i] * Pr[m_1=a_i]}{Pr[c=c_1]} = \frac{1/26*1/26}{1/26} = 1/26$
>
> Similarly, $Pr[m_1 = a_i | c_1 = a_j] = \frac{Pr[c=a_j]|m_1=a_i] * Pr[m_1=a_i]}{Pr[c=c_j]} = \frac{1/26*1/26}{1/26} = 1/26$

> As characters in the message and ciphertext are independent, so $Pr[M = m|C = c] = Pr[m_1 = a_i|c_1 = a_j] * \cdots * Pr[m_n = a_i|c_n = a_j] = 1/26^n$. Because $Pr[M = m] = 1/26^n$, so now we have $Pr[M = m|C = c] = Pr[M = m]$, the cipher is perfectly secret.