- $Pr[K_1] = Pr[K_2] = Pr[K_3] = \frac{\alpha}{3}$ if $\alpha = \frac{1}{3}$ $= \frac{1}{9}$
- $Pr[K_4] = Pr[K_5] = \beta/2$ if $\beta = 2/3$ $= \frac{1}{3}$

To prove perfect secrecy:

$$Pr[\text{Plaintext} \mid \text{ciphertext}] = Pr[\text{Plaintext}]$$

That means the probability of getting a ciphertext is independant of the plaintext and to prove we need to show that for all pairs of plaintexts and for all ciphertexts in C the following holds

$$Pr[\text{plaintext} / \text{ciphertext}] = Pr[\text{Plaintext}]$$

- $Pr[\text{plaintext} = a \mid \text{ciphertext} = 1] = Pr[K_1] + Pr[K_2] = \frac{1}{9} + \frac{1}{9} = \frac{2}{9}$
- $Pr[p = b \mid c = 1] = Pr[K_1] + Pr[K_2] = \frac{1}{9} + \frac{1}{9} = \frac{2}{9}$

- $Pr[p = a \mid c = 2] = Pr[K_3] = \frac{1}{9}$
- $Pr[p = b \mid c = 2] = Pr[K_3] = \frac{1}{9}$

- $Pr[p = a \mid c = 3] = Pr[K_4] = \frac{1}{3}$
- $Pr[p = b \mid c = 3] = Pr[K_4] = \frac{1}{3}$

- $Pr[p = a \mid c = 4] = Pr[K_5] = \frac{1}{3}$
- $Pr[p = b \mid c = 4] = Pr[K_5] = \frac{1}{3}$

All the probabilities are the same for both plaintexts for all possible ciphertexts therefore this means that knowing the ciphertext reveals no information and the system is secure.