Question 1:
Show that the size of the state space of the RC4 cipher is bounded by $2^{16} * 256! \approx 2^{1700}$
Answer:
-Two 8-bit sized indices i and j $\rightarrow (2^8)^2$
-Total amount of 256! permutations for S-box of length 256
$\rightarrow$ Together size of $(2^8)^2 * 256!$

Question 2:
In the RC4 attack, suppose that 60 IVs of the form (3,255,V) are available. Empirically determine the probability that the key byte K_3 can be distinguished.
What is the smallest number of IVs for which this probability is greater than $\frac{1}{2}$?
Answer:
See added Python Code for logic. Probability: Ca 5 %, at least 14 IVs needed

Question 3:
Assuming, that the key bytes K_3 through $K_{\text{n-1}}$ have been recovered, what is the desired form of the IVs that will be used to recover K_{n}?
Answer: $IV = (n, 255, V)$
For K_{n} what is the formula corresponding to 3.11?
Answer:
$KB_{\text{n}} = k_{\text{n}} - \sum_1^n x - V - (\sum_3^{n-1} K_{\text{n}})$

Question 4:
What is the probability that 3.13 holds?
Answer:
K_4: $(\frac{253}{256})^{251} = 0.0518$
What is the probability that the corresponding equation for K_{n} holds?
Answer:
$(\frac{253}{256})^{256\text{-}(\text{n}+1)}$

Question 5:
What is another useful IV for recovering K_3?
Answer::
(3,253,254)
Question 6:
What are other secure methods to employ RC4 when a long-term key is combined with an IV?
Answer:
Increase key size and increase IV size to at least 32-bit (64-bit would be best). Or send the IV encrypted as well.