Part 1:

1. What is the probability that the first two bytes of the plaintext are 0x00 0x02?

   A. The probability of getting the 0x00 and 0x02 is 2^{-16} , which is 1.526 x 10^{-5}.It still depends on the size of the N length size.

2. What is the probability that the next 8 bytes are all non-zero?

   A. The probability of getting next all 8 by bytes non-zeros,

   will be $\left(\frac{255}{256}\right)^{8}$ which is ~ 0.96.

   And as we already know the probability of the 0x00 and 0x002 which will 0.96 * (1.526 x 10^{-5}). Thus, it will be 1.479 x 10^{-5} .

3. What is the probability that at least one of the remaining bytes is zero?

   A. probability of at least one of the remaining bytes is zero will be

$$\left(\frac{255}{256}\right)^{8} * \left(1 - \left(\frac{255}{256}\right)^{118}\right) \approx 0.358$$

4. What is the probability that the plaintext conforms to PKCS #1 v1.5?

   The plaintext conforms to PKCS#1 v1.5 is

$$1.526\text{x}10^{-5}*0.96 * 0.358 \approx 5.46 \text{ x } 10^{-6}$$