Assignment 2:

Part 1:
1. What is the probability that the first two bytes of the plaintext are 0x00 0x02?
0x0002 => 00000000 00000010

A uniformly random plaintext will have a 0.5 chance to have any given bit set. Hence, the probability of this exact sequence for the first two bytes is:
P(0x0002) = (0.5)^16 = 1.52587891×10^−5

2. What is the probability that the next 8 bytes are all non-zero?
The probability that a random byte will be non-zero can be calculated with a binomial distribution:
Chance for success: 0.5
8 trials (one for each bit of the byte)
Probability of a single set bit: P(X>0) = 0.99609375

Now we can use a binomial distribution again to calculate the chance that all 8 bytes are non-zero:
Chance for success: 0.99609375
8 trials (one for each byte)
Probability that all bytes are non-zero: P(X=8) = 0.96917392448

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

1024 bits but we've got 10 bytes so far:
1024 - 80 = 944 bits = 118 bytes

Binomial for at least one zero byte:
Chance for success: 0.99609375
118 trials
P(X<118) = 0.36987692397 * chance for at least one zero byte

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

P(0x0002) * P(8 non-zero) * P(X>0 zero bytes)
(1/2)^16 * (0.96917392448) * 0.36987692397
= 5.46989548 x 10^−6
approximately 5 in a million