Cryptography Assignment 1

Simon Persson, simp, 950307-4511

November 2018

Question 1

The probability that the random block is a xero pad block is $\frac{1}{256}$ since there are 256 possible values and only one of them yields zero pad block.

Question 2

The probability that the random block is a valid pad block has a chance of:

$$\frac{1}{256}+\frac{1}{256^2}+\frac{1}{256^3}+\frac{1}{256^4}+\frac{1}{256^5}+\frac{1}{256^6}+\frac{1}{256^7}+\frac{1}{256^8} = \frac{72340172838076673}{72340172838076673} \approx 0.00392$$

Question 3

$P(A)$: Probability that random block is a zero pad block. This is equal to 0.14 as shown in question 1. $P(B)$: Probability that the random block is valid pad block, which is equal to 0.00392 as shown in question 2. $P(B|A)$ is the probability that a pad block is valid given that we have a zero pad block. Since we have a zero pad block we also have a valid pad lock and thus is $P(B|A) = 1$.

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)} = \frac{1 * 0.14}{0.00392} = 0.996$$

Question 4

$$D(c) \oplus (R_i \oplus C') = D(E(P \oplus C')) \oplus (R_i \oplus C') = P \oplus C' \oplus R_i \oplus C' = P \oplus R_i$$

Question 5

Since we know that the last byte of $P \oplus R_i$ is zero which implies that $i \oplus P_8 = 0$. That means that $i = P_8$ since anything xor:ed with itself is zero.

Question 6

Since we decode P from LSB to MSB we do not want to add anything to the "right" of P but only to the "left". Furthermore it is a good idea to only add zeroes so we know that no information gets lost.

Question 7

If the padding is correct we know that the last two bits of the message should be 1. Therefore we we can obtain b_7 by

$$b - 7 \oplus 1 = 1$$

$$b_7 = i \oplus 1$$

.

Question 8

Following the previous structure the message to find b_6 has the form:

$$< r_1, r_2, r_3, r_4, r_5, i, b_7 \oplus 2, b_8 \oplus 2 >$$