Cryptography module, Answers 1

1. Initially, we have $L_0 = 86$, $R_0 = 83$, $K_0 = 89$. Then we run the first round, to obtain $L_1 = 83$, $R_1 = 2$. Also, $K_1 = 164$. So, computing the next round, we have $L_2 = 9$ and $R_2 = 2$. So the output is $(9, 2)$.

2. In both cases, the block cipher is not secure. We could guess that because it is so simple (why would we need DES or AES if we could get a secure block cipher as simply as the question suggests?). Formally, to demonstrate it is not secure, we need to give a *strategy for the attacker* based on the Block Cipher Game[1]. A strategy for the attacker consists of the queries it will make of the challenger, and the computations it will do based on those queries, and the output of its guess as to whether the challenger is running a random permutation or the block cipher.

   (a) There are several strategies for the attacker that will work. One such is: the attacker chooses any two messages x and y, and obtains the answers $g(x)$ and $g(y)$. Then s/he computes $x \oplus y$ and $g(x) \oplus g(y)$. These values would be the same if the challenger is running the block cipher, since $g(x) \oplus g(y) = k \oplus x \oplus k \oplus y = x \oplus y$. If these two values are different, the attacker reasons that the challenger cannot be using the block cipher, and outputs its guess accordingly. If the two values are the same, the attacker reasons that the challenger is very likely to be running the block cipher, because it is very unlikely that a random permutation would result in the values being the same, and outputs its guess accordingly.

   If the attacker outputs that s/he thinks the challenger is using a random permutation, s/he is certainly right. If s/he outputs that s/he thinks the attacker is using the block cipher, the probability s/he is wrong is $1/2^n$, where n is the bitlength of the strings. In both cases, s/he has a significant (and thus, non-negligible) probability of being right.

   (b) Again, several answers are possible. One such is: the attacker choses two messages that differ only in the first bit, and submits them to to the challenger. Suppose m_0 starts with the bit 0, and m_1 is idential but starts with the bit 1. Then $m_0 - k \bmod 2^{128}$ and $m_1 - k \bmod 2^{128}$ are also identical except for the first bit, and so are $(m_0 - k \bmod 2^{128}) \oplus k$ and $(m_1 - k \bmod 2^{128}) \oplus k$. The attacker therefore compares these values. If they are identical except for the first bit, s/he concludes the challenger was using the block cipher. If they are not, s/he concludes the challenger is using a random permutation.

3. (a) 3628010628.

   (b) After multiplying, we get $x^5 + x^2 + x + 1$. Note that there were two x^3 terms during the calculation, but since the coefficients are treated modulo 2, and $1 + 1$ equals 0 mod 2, there is no x^3 term at the end of the multiplication. Next, we want to reduce this modulo $x^4 + x + 1$. We find that $x^5 + x^2 + x + 1$ is equal to $x(x^4 + x + 1) + 1$, so the final answer is 1.

[1] Slide 39 of the lecture notes, or see `https://en.wikipedia.org/wiki/Block_cipher#Standard_model` (accessed 31 October 2017)

4. (a) Insecure. For example, an attacker would be able to detect if the first two plaintext blocks are the same, i.e., whether $m_1 = m_2$, by checking if $c_0 = c_2$. (To see this, note that $c_2 = E(k, m_2) \oplus c_1 = E(k, m_2) \oplus E(k, m_1) \oplus c_0$. If $m_1 = m_2$ then the two E terms cancel out, and $c_0 = c_2$.)

   To show that the mode of operation is insecure with respect to the security definition IND-CPA[2], we need to give a strategy for the attacker. A suitable strategy would be this: submit two messages, the first one having identical first two blocks, and the second one having non-identical first two blocks. Then we can see which encryption comes back, by performing the test indicated above.

   (b) Insecure. This mode suffers from the same problem: the attacker can detect if two blocks of the plaintext are the same. Therefore, the same strategy for the attacker to win the game will work here.

5. In hex notation, the first 20 bytes are:
   97 36 8F 68 42 95 C4 B4 99 AD 8F 8 38 8C C2 B0 71 1F 62 DD.

6. The idea was to add a photo of yourself to your Canvas profile. Many people did that, but some people just attached a photo to their answers to the cryptography exercise instead of adding it to their profile. If you did that, please add it to your profile instead.

[2] Slide 85-87.