Cryptography module, Exercises 1 (assessed)

You must type your answers in a word processing system, and create a PDF. I cannot accept handwritten and scanned or photographed answers. Please submit your PDF on Canvas. The maximum mark you can get is 10 (if you get 11, it will be capped at 10). The deadline for these exercises is 23 October 2017.

You can work on your own, or you can work in pairs. If you work in a pair, only one of you should submit the answers (of course, both will get the credit). Please note on your answers that you worked as a pair, and please mention both ID numbers.

1. Assume a simple two round Feistel block cipher with an 8 bit key and 16 bit block size. We have two rounds, with $i = 0$ and $i = 1$, and two round keys. The round keys are defined as $K_i = K + 75 \times i \pmod{256}$. The Feistel function is $f(K_i, R_i) = 127 \times (K_i + R_i) \pmod{256}$, where R_i is the decimal representation of the right 8 bits of the input block.

   Encrypt the message block $M = (\texttt{V}, \texttt{S})$ with key $K = \texttt{Y}$. Use the ASCII encoding of capital letters where `A` is encoded as 65. It is sufficient to give your result as a pair of decimal numbers. **[2%]**

2. For each of the following block ciphers E_1 and E_2, explain whether the cipher is a *secure* pseudorandom permutation. (In both cases, the key size and the block size are 128 bits.)

   (a) $E_1(k, m) = k \oplus m$.

   (b) $E_2(k, m) = (m - k \bmod 2^{128}) \oplus k$. **[2%]**

3. Compute the following:

   (a) $1234567890 \times 5678901234 \bmod 7890123456$.

   (b) $(x^2 + 1)(x^3 + x + 1) \bmod x^4 + x + 1$. **[2%]**

4. Let E be a secure block cipher (say, AES). Consider each of the following modes of operation. For each one, say whether it is secure or not, and briefly explain your answer.

   (a) The encryption by k of $m_1||m_2||\ldots||m_n$ is $c_0||c_1||c_2||\ldots||c_n$, where c_0 is a randomly chosen "initialisation vector" of appropriate size, and $c_i = E(k, m_i) \oplus c_{i-1}$ $(i > 0)$.

   (b) The encryption by k of $m_1||m_2||\ldots||m_n$ is $N||c_1||c_2||\ldots||c_n$, where N is a randomly chosen nonce of appropriate size, and $c_i = E(k, N \oplus m_i)$. **[2%]**

5. Find the first 20 bytes of the output of the RC4 algorithm when run with the key $K = [1, 2, 3]$. **[2%]**

6. Add a photo of yourself to Canvas. This helps staff members match their verbal discussions with you with their Canvas interactions. **[1%]**