Coursework 4

Computer Processors (XJCO1212)

You should follow the instructions below on how to prepare your submission. Late submissions are accepted up to 7 days late. Each day, or part of a day, will incur a 5% penalty. Feedback on late submissions may not be provided within 3 weeks of submission.

Submission You **must** submit your work via Gradescope.

Deadline **1000 GMT 10/05/2021**.

Weighting This piece of summative coursework is worth 25% of the module grade.

The Feistel cipher is a symmetric block cipher encryption framework which is the basis of many modern day encryption algorithms. In this coursework you will implement a Feistel cipher system as a hardware component and as a software implementation. In a Feistel cipher the plaintext, P, to be encrypted is split into two equal size parts L_0 and R_0 such that $P = L_0R_0$. A function F is applied to one half of the plaintext, combined with a key, and the result is XOR'd with the other half of the plaintext. Feistel ciphers often employ multiple rounds of this scheme. In general the scheme works as follows, for all $i = 0, \dots, n$,

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus F(R_i, K_i) \end{aligned}$$

To decrypt an encrypted message using this cipher we can apply the same procedure in reverse. For $i = n, n-1, \dots, 0$,

$$\begin{aligned} R_i &= L_{i+1} \\ L_i &= R_{i+1} \oplus F(L_{i+1}, K_i) \end{aligned}$$

For this coursework we are interested in the 16-bit Feistel cipher which uses 4 rounds. The function $F(A, B) = A \oplus B$. The keys are derived from a single 8-bit key K_0 such that,

$$\begin{aligned} K_0 &= b_7b_6b_5b_4b_3b_2b_1b_0 \\ K_1 &= b_6b_5b_4b_3b_2b_1b_0b_7 \\ K_2 &= b_5b_4b_3b_2b_1b_0b_7b_6 \\ K_3 &= b_4b_3b_2b_1b_0b_7b_6b_5 \end{aligned}$$

1. Produce an implementation, in HDL, of the described Feistel encryption scheme. The chip should have the following preamble.

   ```
   CHIP FeistelEncryption {
       IN plaintext[16], key[8];
       OUT ciphertext[16];

       PARTS:

   }
   ```

2. Write a program in HACK assembly, without using symbols, that implements the described Feistel encryption system. The initial key, K_0, will be stored in RAM[1], and the 16-bit plaintext will be stored in RAM[2]. The result of the encryption should be stored in RAM[0].

Question 1 is worth **10 marks**, and Question 2 is worth **15 marks**.