CM30173: Example sheet 3

6th February

Questions 1 relates to lecture 4. Question 2 relates to lecture 5.

1. Take the SPN from lectures and replace the S-boxes with:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F

   For the resulting SPN:

   (a) Find the row of the difference distribution table corresponding to input difference 1110

   (b) Calculate the full difference distribution table (not by hand!)

   (c) Describe a differential attack on this SPN, you should aim to find a differential trail which has propagation ratio $\frac{81}{4096}$ (I believe that there are a variety of these).

   (d) Implement your attack (you will need to use your SPN implementation to encrypt your chosen plaintext-ciphertext pairs).

2. Give the definition of a Feistel cipher. Explain why we do not require f to be injective and describe the decryption algorithm.