CS 741 Assignment 2

Due Date 14/03/21

1. Write a program to compute the bias of each combination of inputs and outputs to/from the AES S-Box (note that each combination should include at least one of the 8 inputs and at least one of the 8 outputs). Plot a histogram of the biases and also include a table showing the biases and the number of combinations with that bias. (The biases should be positive (even – why?) integers).

   Input:
   There is no input and you can hard-code the AES substitution box in your code.

   Output:
   Your code should output the table showing the biases and the number of combinations with that bias.
   If you're using a different code to plot the histogram, submit that too.

   Report:
   Add a **report.pdf** file that includes the **bias table** and the **histogram**.
   Also, state the time complexity in numerical format eg.
   $O(2^{10} * 2^{14} *\ldots) = O(2^{56})$ and the approx. time your program takes to complete.

2. Given an $s \; x \; s$ S-Box, the number of stages in the SPN (Substitution Permutation Network), and the plaintext/ciphertext block size, write a program to obtain a linear expression with the maximum possible bias. The expression should be an XOR of bits of the plaintext, bits of the ciphertext, and bits of the round keys (all but the last round).

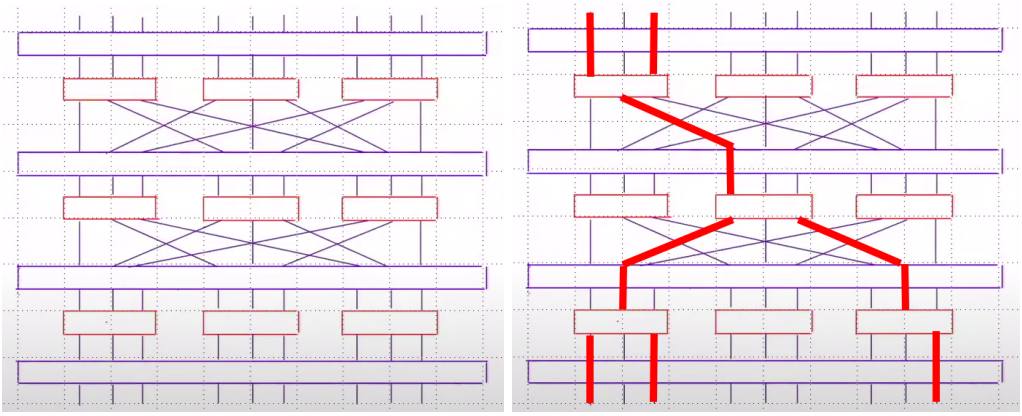
   2.1 *"A greedy strategy will always work."* Examine the validity of this claim.

   Input:
   $Num\ of\ stages\ (T)$
   $Size\ of\ plaintext\ (N)$
   $Permutation\ (of\ size\ N,\ space\ separated)$
   $Size\ of\ S\ -\ box\ (S)$
   $S\ -\ box\ (\ of\ size\ 2^S)$

   Output:
   Print the bits which give the maximum bias and if possible, the value of the bias too.
   (maximum bias above means bias with maximum absolute value, so -½ is better than ¼)

   Report:
   Add a **report.pdf** file that explains your algorithm.
   State the conclusion for the above claim(2.1) and a brief explanation for the same. *(How did you reach the conclusion?)*
   Also, state the time complexity eg. $O(T * N^2 * 2^S *\ldots)$.

Example: (The output is completely random just to explain the format)



Input:

3 ## the last round-key operation is not considered as round
9
0 3 6 1 4 7 2 5 8 ## 0 mapped to 0, 1 mapped to 3, 2 mapped to 6 ...
3
0 2 4 6 3 1 7 5 ## 0 - 0, 1 - 2, 2 - 4 … substitution

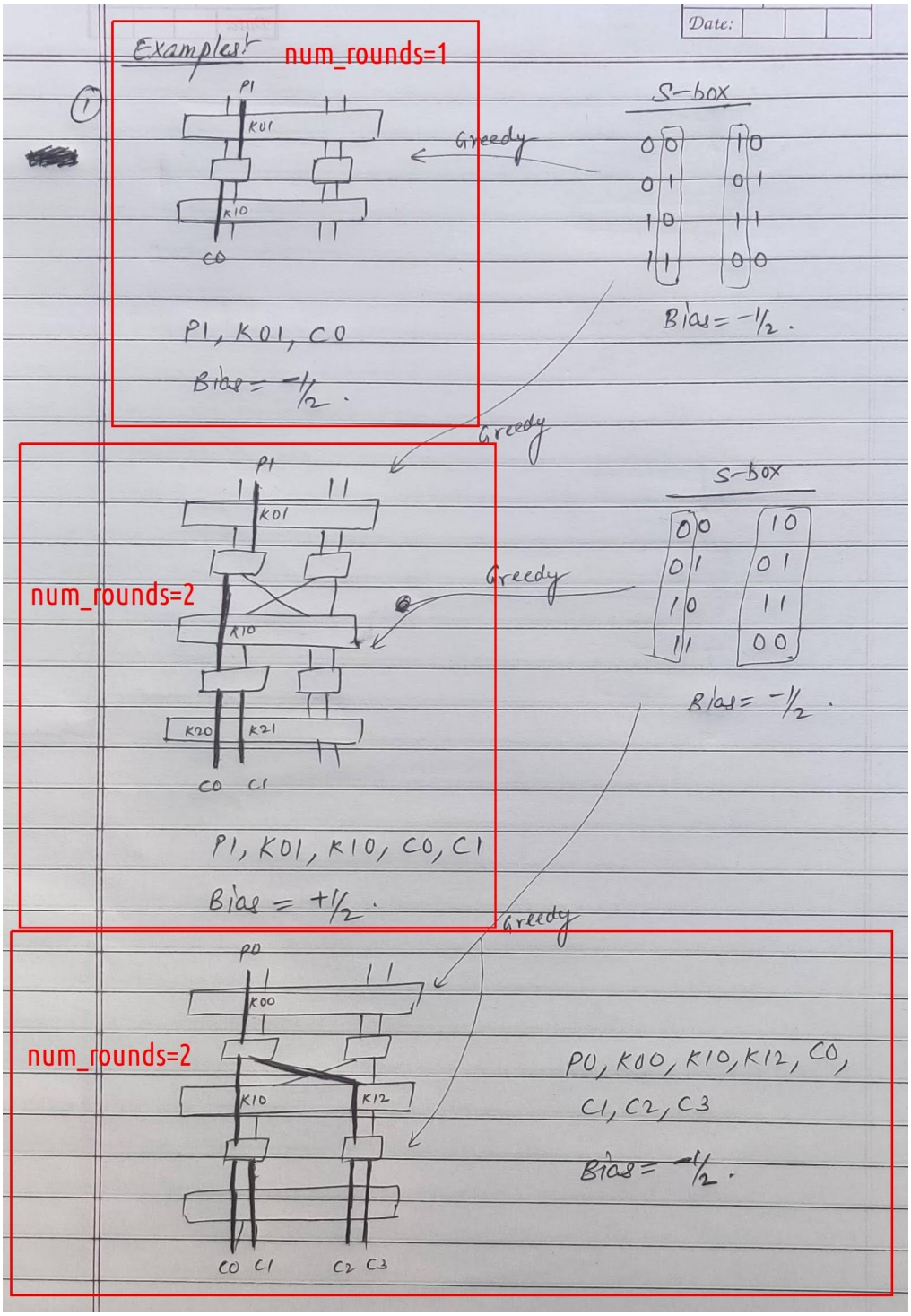
Output:

P0, P2, K00, K02, K13, K21, K27, C0, C2, C8
Bias = 0.125

The correct bias for the above path is 0 because of the 2nd S-box.

(There is no need to follow the strict output convention, something similar to the above output will suffice. Add the format in the report.)

These are 3 simple examples to test your understanding and code:



Greedy strategy worked for all cases above. But this does not claim anything.

3. **(Extra Credit)** Implement Step 2 of the linear cryptanalysis attack to deduce bits of the last round key.

   Same input format as above with some additional plaintext/ciphertext pairs.

   Report:
   Add a **report.pdf** file that explains your algorithm and the input/output format you're assuming for the plaintext/ciphertext pairs.
   Also, add the output format for the last-round key.

Submission Instructions:

- Create a folder named <Roll1_Roll2_Roll3_Roll4> with 3 sub-directories Q1, Q2, and Q3.
- There should be code and a report (named **report.pdf**) for each of the 3 questions (in respective sub-directories).
- Submission must be made from only the least lexicographical roll number. The name of the submitted zip file should be "Roll1_Roll2_Roll3_Roll4.zip" eg: 170050001_170050002_170050003_170050004.zip