CSI4108 / SEC5101
(Fundamentals of) Cryptography

Cryptanalysis Project
Due: Wednesday, November 6, 2024 (before 16:00, to be submitted via Brightspace)

To be done in teams of 2; please find a partner among your classmates.

[3 marks] The team members will together randomly generate an s-box *S* and analyze it to construct its Difference Distribution Table (similar to Table 7 in Heys' paper) and find the best Differential Characteristic (similar to Figure 5 in the paper). Show your s-box and describe all your analysis.

(a) Person 1 will randomly generate five 16-bit round keys (the round keys are to be kept secret) and will then encrypt 10,000 known 16-bit plaintext strings, resulting in 10,000 corresponding 16-bit ciphertext strings. Person 2 will follow the process described in Heys' tutorial for differential cryptanalysis to compute a table similar to Table 8 in order to learn one byte of the final round key. Once Person 2 has determined this alleged key byte, Person 1 will reveal the actual key byte used.

(b) Person 1 and Person 2 will then switch roles and repeat Step (a).

[2.5 marks] Discuss all aspects of the attack by Person 2 in Step (a).

[2.5 marks] Discuss all aspects of the attack by Person 2 in Step (b).