MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 3: Problems for Homeworks 3 and 4

Problem 1. Consider the following S-box with 3 input bits and 3 output bits (a 3×3 S-box):

Input:	000	001	010	011	100	101	110	111
Output:	110	101	001	000	011	010	111	100

(a) Make a linear approximation table for this S-box, analogous to Table 4 in Heys.

(b) What is the highest probability bias (either positive or negative) of any input sum and output sum?

Problem 2. Consider the simple substitution permutation network shown in Figure 1 at the end of this handout. Assume that the S-box used is that from Problem 1. Find the encryption of the plaintext "011010", using the key $(K_1, K_2, K_3, K_4) = (010101, 001011, 111000, 111110)$. For convenience, also show the intermediate results (i.e., the rows A, B, D, E, F, G, H, and J from Figure 1).

Problem 3. For the substitution permutation network from Problem 2:

(a) Find a linear approximation, analogous to Figure 3 in Heys, which relates the plaintext bits P_1, P_2, P_4, and P_5 to a suitable subset of the inputs to the last round of S-boxes, i.e., a subset of the bits $H_1, \ldots, H_6$.

(b) What is the total bias of the linear approximation you found in part (a)? What does this mean?

(c) Suppose you are given the following known plaintext/ciphertext pairs for this cipher, all encrypted with the same (unknown) key:

Plaintext	Ciphertext
100111	100100
000111	110010
001100	111001
011000	011101
001000	001101
011010	101001

Using the linear approximation from part (a), determine the first and third bits of the subkey K_4. (Bonus question: why is this information insufficient to determine the second bit of the subkey K_4?)

NOTE: this problem has been specifically constructed so that a very small number of plaintexts and ciphertexts is sufficient to determine two subkey bits. Unlike the general method of Heys, a probabilistic analysis is not necessary in this problem — the bits in question can be determined with certainty.

Problem 4. Make a difference distribution table, analogous to Table 7 in Heys, for the S-box from Problem 1.

Problem 5. For the substitution permutation network from Problem 2: Consider two plaintexts P and P' such that $\Delta P = P \oplus P' = 000001$.

(a) Using your difference distribution table from the previous problem, what are the possible values for ΔH? Remark: note that there are only six possible values.

(b) Suppose you are given the following additional chosen plaintext, and corresponding ciphertext:

Plaintext	Ciphertext
100110	111110
000110	110110
001101	100000
011001	011111
001001	000011
011011	101000

This is in addition to the plaintext/ciphertext pairs from Problem 3. Use your answer to part (a) to determine the last three bits of the subkey K_4.

NOTE: this problem has been specifically constructed so that a very small number of plaintexts and ciphertexts is sufficient to determine three subkey bits. Unlike the general method of Heys, a probabilistic analysis is not necessary in this problem — the bits in question can be determined with certainty.

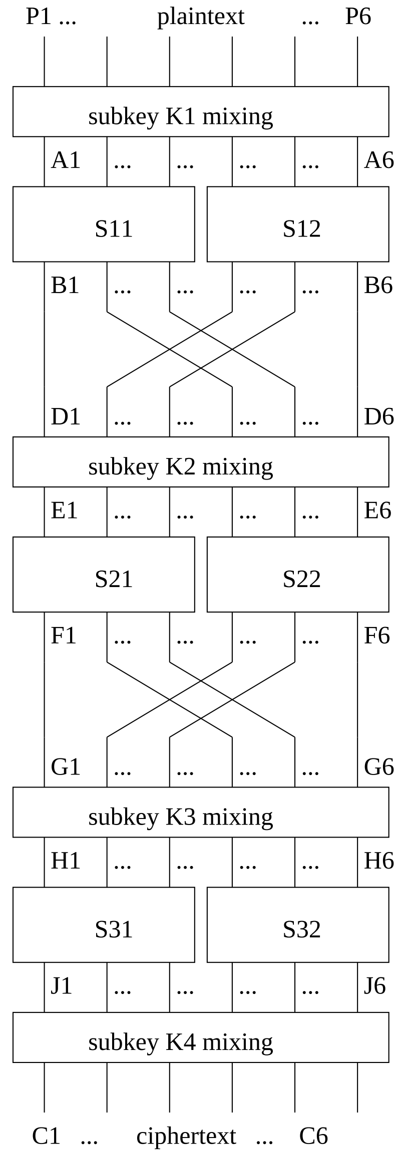

Figure 1: A very simple SPN network