COMP547B Homework set #4

Due Monday March 27th, 2017

Exercises (from Katz and Lindell's book)

Read sub-section "Attacks on reduced-round substitution-permutation networks" on pages 168—170 before solving question 5.2:

[15%] 5.2 In our attack on a two-round substitution-permutation network, we considered a block length of 64 bits and a network with 16 S-boxes that each take a 4-bit input. Repeat the analysis for the case of 8 S-boxes, each taking an 8-bit input. What is the complexity of the attack now? Repeat the analysis again with a 128-bit block length and 16 S-boxes that each take an 8-bit input. Does the block length make any difference?

5.5 What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

[5%] (a) Each round function outputs all 0s, regardless of the input.

[5%] (b) Each round function is the identity function.

[10%] 5.6 Show that DES has the property that $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ for every key k and input x (where $\overline{z}$ denotes the bitwise complement of z). This is called the *complementarity property* of DES. (The description of DES given in this chapter is sufficient for this exercise.)

[10%] 5.8 In the actual construction of DES, the two halves of the output of the final round of the Feistel network are swapped. That is, if the output of the final round is (L_{16}, R_{16}) then the output of the cipher is in fact (R_{16}, L_{16}). Show that the only difference between the computation of DES_k and DES_k^{-1} (given the swapping of halves) is the order of subkeys.

5.9 (This exercise assumes the results of the previous exercise.)

[5%] (a) Show that for $k = 0^{56}$ it holds that $DES_k(DES_k(x)) = x$. Why does the use of such a key pose a security threat?

[5%] (b) Find three other DES keys with the same property. These keys are known as *weak keys* for DES.

[5%] (c) Does the existence of these 4 weak keys represent a serious vulnerability in DES? Explain your answer.

More on back…

5.10 Describe attacks on the following modifications to DES:

[5%] (a) Each round sub-key is 32 bits long, and the mangler function simply XORs the round sub-key with the input to the round (i.e., $\hat{f}(k, R) = k_i \oplus R$). For this example, the key schedule is unimportant and you can treat the k_i as independent keys.

[5%] (b) Instead of using different sub-keys in every round, the same 48-bit sub-key is used in every round. Show how to distinguish the cipher from a random permutation without a 2^{48}-time brute-force search.

Hint: Exercises 5.8 and 5.9 may help...

5.12 This question illustrates an attack on two-key triple encryption. Let F be a block cipher with n-bit block length and key length, and set $F'_{k_1,k_2}(x) = F_{k_1}(F^{-1}_{k_2}(F_{k_1}(x)))$.

[5%] (a) Assume that given a pair (m_1, m_2) it is possible to find in *constant* time all keys k_2 such that $m_2 = F^{-1}_{k_2}(m_1)$. Show how to recover the entire key for F' (with high probability) in time roughly 2^n using three known input/output pairs.

[5%] (b) In general, it will *not* be possible to find k_2 as above in constant time. However, show that by using a pre-processing step taking 2^n time it is possible, given m_2, to find in (essentially) constant time all keys k_2 such that $m_2 = F^{-1}_{k_2}(0^n)$.

[5%] (c) Assume k_1 is known and that the pre-processing step above has already been run. Show how to use a single pair (x, y) for a *chosen* input value x to determine k_2 in constant time.

[5%] (d) Put the above components together to devise an attack that recovers the entire key by running in roughly 2^n time and requesting the encryption of roughly 2^n chosen inputs.

[10%] 5.14 Say the key schedule of DES is modified as follows: the left half of the master key is used to derive all the sub-keys in rounds 1–8, while the right half of the master key is used to derive all the sub-keys in rounds 9–16. Show an attack on this modified scheme that recovers the entire key in time roughly 2^{28}.