MATH 195: CRYPTOGRAPHY
HOMEWORK #5

Problem 3.15. *In SDES, a key* $K = (k_1, \ldots, k_{10}) \in \mathbb{F}_2^{10} = (\mathbb{Z}/2\mathbb{Z})^{10}$ *gives rise to two subkeys* $K_1, K_2 \in \mathbb{F}_2^8$. *Express* K_1 *and* K_2 *directly in terms of* K. *[Hint: Use the text, pp. 52–53.]*

Problem 3.1. *Refer to Figure 3.2, which depicts key generation for SDES.*

(a) *How important is the initial P10 permutation function?*
(b) *How important are the two LS-1 shift functions?*

Problem 3.3. *Using SDES, decrypt the string* (10100010) *using the key*

$$(0111111101)$$

by hand. Show intermediate results after each function $(IP, F_K, SW, F_K, IP^{-1})$. *Then decode the first 4 bits of the plaintext string to a letter and the second 4 bits to another letter where we encode A through P in base 2 (i.e.,* $A = 0000$, $B = 0001$, $\ldots$, $P = 1111$*). [Hint: As a midway check, after the application of* SW, *the string should be* (00010011)*.]*

Problem 3.16. *In DES, one has* $K_i = \tau\lambda^{n_i}\sigma(K)$ *for* $1 \leq i \leq 16$ *with* τ, λ, σ *and* $n_1, \ldots, n_{16}$ *as explained in class. Prove:* $K_{17-i} = \tau\rho^{n_i-1}\sigma(K)$, *where* $\rho = \lambda^{-1}$. *From which property of Table 3.4(c) does this follow?*

Date: February 26, 2002.
3.15, 3.1, 3.3, 3.16.