

CSE 651 Homework 2

Due: Monday, April 19 by class time

1. Do Problem 3.2 of Stallings. (Hints: (1) The information about 128-bit block size and key length is not important. (2) Imagine that there is an oracle who can encrypt one message of your choice for you; this question asks how you can make use of this oracle to decrypt your ciphertext c .)
2. Do Problem 3.7 of Stallings. Hints: (1) in the 4th edition, the symbol \otimes in the question should be \oplus , XOR; this has been corrected in the 5th edition. (2) The function computed by the modified DES is: $IP^{-1} \circ \mu \circ \psi \circ IP(m)$, where m is a plaintext block, μ is the swap function defined in class, IP is the initial permutation, IP^{-1} is the inverse initial permutation, ψ is the 16 rounds. Here you need to figure out the function ψ . You should not simply answer that $\psi = \mu \circ \phi_{16} \circ \dots \circ \mu \circ \phi_2 \circ \mu \circ \phi_1$.
3. Do Problem 3.12 of Stallings. In addition to specifying a table analogous to Table 3.4d, you need to indicate whether to rotate to the left or to the right.
4. Consider AES. (a) Suppose we change one bit in the first byte of the input block. After the first round of AES, how many bits of the output matrix *state* are possibly affected? (b) Answer the same question but now we change one bit in the last byte of the input block.