

Computer Science 427/527 Computer Security  
Homework # 2  
Assigned: Jan 22, 2007  
Due: Jan 29, 2007

Problem 1. (30 points). Decrypt the following SDES encryption by hand.  
(Hint: Remember that decryption runs backwards.)

Ciphertext = 00011000  
Key = 1000000001

Show the following intermediate results:

- Part a. (2 points).      After P10
- Part b. (4 points).      Subkey K1
- Part c. (4 points).      Subkey K2
- Part d. (4 points).      After Initial permutation
- Round 1 begins
- Part e. (4 points).      Input to P4 (combined output of S-boxes)
- Part f. (4 points).      Switch output
- End of round 1
- Part g. (4 points).      Input to P4 (combined output of S-boxes)
- Part h. (4 points).      Plaintext