MCS 425 Exercise Set #5 — Spring Semester, 2008

Section 18.12, exercises 1, 3, 4, 5

Exercise P. Alice and Bob have public and private RSA keys as follows:

Alice:	$(n_A, e_A) = (95,7)$,	$d_A = 31$
Bob:	$(n_B, e_B) = (77,47)$,	$d_B = 23$

a) Alice receives two messages, digitally signed using the RSA, both claiming to be from Bob, but one is a forgery. The messages are (33,2) and (27,48). Which message is the forgery, and why?

b) Alice wants to send the reply message 38 to Bob, encrypted *and* digitally signed. What values does she actually transmit to Bob?