Introduction to Cryptography  
Problem Set 7  
Due: Tuesday, April 13


2. Stallings, 9.3.


4. Alice submits a bid to an auction, and so that other bidders cannot see her bid, she encrypts it under the public key of the auction service. Suppose that the auction service provides a public key for an RSA encryption scheme, with a modulus $n$. Assume that bids are encoded simply as integers between 0 and $n - 1$ prior to encryption. Also, assume that Alice submits a bid that is a “round number,” which in this case means that her bid is a number that is divisible by 10. Show how an eavesdropper can submit an encryption of a bid that undercuts Alice’s bid by 10%, without even knowing what Alice’s bid is. In particular, your attack should work even if the space of possible bids is very large.