Cryptography & Network Security

(2015/11/9) Midterm I

1. Define the three security goals.
2. List and define five security services.
3. We have been told in arithmetic that the remainder of an integer divided by 8 is the same as the remainder of division of the rightmost three digits by 8. Use the properties of the mod operator to prove this claim.
4. Using the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of *s* and *t*.
   (a) 84 and 320
   (b) 400 and 60
5. Find the multiplicative inverse of each of the following integers in $\mathbf{Z}_{180}$ using the extended Euclidean algorithm.
   (a) 7
   (b) 132
6. A post office sells only 39-cent and 15-cent stamps. Find the number of stamps (for 39-cent and 15-cent stamps, respectively) a customer needs to buy to put $ 2.70 postage on a package. Find all possible solutions.
7. The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key.
8. Find all subgroups of the following groups:
   (a) G= < $\mathbf{Z}_{16}$, +>
   (b) G= < $\mathbf{Z}_{16}^{*}$, *>
9. For the group G=< $\mathbf{Z}_4$, +>, prove that it is an abelian group.
10. Alice uses three consecutive permutations [1 3 2], [3 2 1], and [2 1 3]. Show how Bob can use only one permutation to **reverse** the process.