Homework 1

Please put your solutions in a .doc or .pdf to CSNS by 11:59pm, Saturday 02/01.

Total points: 5

---

1 (0.5pt). What integers do the sets Z_{28} and Z_{28*} contain? For each set, list all additive inverse pairs and multiplicative inverse pairs.

---

2 (1pt). Using extended Euclidean algorithm, show the steps of finding the following multiplicative inverses

a) 321^{-1} mod 56709.

b) 345^{-1} mod 76408

3(1pt). Find the all solutions to each of the following linear equations

a) $24x \equiv 12 \pmod{28}$

b) $4x + 5 \equiv 17 \pmod{10}$

c) $5x \equiv 15 \pmod{25}$

d) $24x + 20 \equiv 29 \pmod{69}$

---

4 (0.5pt). Encrypt the message "do not attack" using the following ciphers. Ignore the space between the words. Decrypt the message to get the original plaintext. (note: please ignore the spaces)

a). Additive cipher with key = 12

b). multiplicative cipher with key = ~~11~~ 15

c). Affine cipher with key = (15,12)

5.(1pt). a) Construct a Playfair key matrix with the keyword "university"
b) Use the matrix created in a) to encrypt the message "attackistomorrow"

---

6. (0.5pt). The encryption key in a transposition cipher is
(5, 12, 3, 7, 9, 6, 4, 14, 1, 13, 10 , 8, 15, 2, 11,16).
Find the decryption key

7. (0.5pt) Show that an integer N is congruent modulo 9 to the sum of its decimal digits. For example, $475 \equiv 4+7+5 \equiv 16 \equiv 1+6 \equiv 7 \pmod 9$.