Cryptography and Network Security

(Midterm II; 2013/12/02)

1. Encrypt the message "this is an exam" using one of the following ciphers. Ignore the space between words. What are their ciphertext (in character form), respectively?
   a. Additive cipher with key = 8
   b. Multiplicative cipher with key = 5

2. The encryption key in a transposition cipher is (3, 1, 5, 2, 6, 4). Find the decryption key.

3. Find all subgroups of the following groups:
   a. $G = \langle Z_{15}, + \rangle$
   b. $G = \langle Z_{15}^*, x \rangle$

4. A transposition block has 8 inputs and 8 outputs. What is the order of the permutation group? What is the key size?

5. A substitution block has 8 inputs and 8 outputs. What is the order of the permutation group? What is the key size?

6.
   a. Swap the word $(10011011)_2$.
   b. Swap the word resulting from Part a.
   c. Is swapping is a self-invertible operation? Why?

7. Alice can use only the additive cipher on her computer to send a message to a friend. She thinks that the message is more secure if she encrypts the message two times, each time with a different key. Is she right? Defend your answer.

8. Alice has a long message to send. She is using the monoalphabetic substitution cipher. She thinks that if she compresses the message, it may protect the text from single-letter frequency attack by Eve. Does the compression help? Should she compress the message before the encryption or after the encryption? Defend your answer.

9. (a) Find the result of $00100110 \otimes 10011110$ in $GF(2^8)$ with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.
   (b) Find the inverse of 00100110 in $GF(2^8)$ with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.

10. A 6×2 S-box exclusive-ors the odd-numbered bits to get the left bit of the output and exclusive-ors the even-numbered bits to get the right bit of the output. If the input is 110010, what is the output? If the input is 101101, what is the output?