# Cryptography & Network Security

(2015/12/21) Midterm II

1. For each of the following *n*-bit words, find the polynomial that represent that word:
   (a) 100001
   (b) 00011
2. Find the *n*-it word that is represented by each of the following polynomials:
   (a) $x^2+1$ in GF($2^4$)
   (b) $x^7$ in GF($2^8$)
3. Find the multiplicative inverse of the following polynomials in GF($2^2$). Note that there is only one modulus for this field.
   (a) $x+1$
   (b) $x$
4. Determine whether the P-box with the following permutation table is a straight P-box, a compression P-box, or an expansion P-box.
   (a) [1 2 3 4 5 6]
   (b) [1 3 5 6 7]
5. (a) A substitution block has 10 inputs and 10 outputs. What is the order of the permutation group?
   (b) A transposition block has 10 inputs and 10 outputs. What is the order of the permutation group?
6. (a) Which of the four transformations defined for AES change the contents of bytes?
   (b) Which one does not change the contents of bytes?
7. Describe the Ciphertext Stealing Technique for CBC mode.
8. A 6X2 S-box exclusive-ors the odd-numbered bits to get the left bit of the output and exclusiver-ors the even-numbered bits to get the right bit of the output. If the input is 111010, what is the output? If the input is 101001, what is the output?
9. Use the extended Euclidean algorithm to find the inverse of $(x^4+x^2+1)$ in GF($2^5$) using the modulus $(x^5+x^2+1)$.
10. Discuss Error Propagation for CBC, ECB, CFB, OFB, and CTR modes.