Cryptography and Network Security

(Midterm 2010/11/29)

1. Find the determinant and the multiplicative inverse of the following residue matrix A over Z_{10}. $\mathbf{A}= \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$

2. Find all solutions to the following sets of linear equations:

   (a) $7x+3y \equiv 3 \pmod 7$
   $4x+2y \equiv 5 \pmod 7$

   (b) $2x+3y \equiv 5 \pmod 8$
   $x+6y \equiv 3 \pmod 8$

   (6, 1)

3. 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.

4. 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.

   no

5. (a) Find the result of 00100110 ⊗ 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 $x^8+ x^4+ x^3+ x+ 1$.

   x^7 x x

6. 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?

7. What is the key complement property in DES? How can you use this property to perform brute-force attack in 2^{55} encryptions instead of 2^{56} encryptions?

8. What's the purpose of Ciphertext Stealing Technique? How can it be applied to EBC mod and CBC? mode

9. (a) A full-size key *n*-bit transposition cipher can be modeled as a permutation. What's its key length? Defend your answer.

   (b) A full-size key *n*-bit substitution cipher can be modeled as a permutation. What's its key length? Defend your answer.

10. List the parameters (block size, key size, and the number of rounds) for the three AES versions.

x^5

111000
111

1000101 1011) 100010110
1000110
1101

111111
111111
1000001

1001000
1111
1010111
1010111
10010
1000101

x^8+x^4

111000
111
111110

1 100110) 100011011
100110
101011
100110
1101

1101) 100110
1101
1001
1101
1000
1101
101

54

1111100
111110
1000100
111110
1011010

1101
11
111
101

$x^5+x^4+x^3$

1111100
111110
1000010

100
1010110
111110
1010100