CSMC 456

Homework #1

Due date: Wednesday September 13th

1) Encrypt the following message with the one-time pad using the given-key
k = 101100001101
m = 011010110001

2) After learning that one of the enemies sent the message "we attack in a week" encrypted as "DWFTABWDUMAWDXS" 6 days ago, your allies have just intercepted a ciphertext which contains the information of whatever the enemy is going to attack by land or by sea. Can you figure which it is? (Assume that the encryption scheme is secure for fixed length messages).

FMAKFINQNFMWQH

(Hint: Notice that the lengths of the ciphertexts are different and that we have already seen the type of message that may be sent).

3) Is it possible to use a shorter key to encrypt longer messages with perfect security. (Consider the size of the message space), give an explicit example.

4) Authenticate the following message using the one-time mac.
p = 23
m = 11
k = (12,5)

5) Authenticate the following message using the one-time mac.
p = 23
m = (11,4)
k = (14,2)

6) Consider that Jon (who knows nothing) selected p=32 for the parameter of a one-time mac. Show how an enemy can successfully forge a mac tag knowing that 14 is a valid mac tag on the value 0.
p = 32
m = 0
t = 14

7) Dave and Evan each have a proposal to authenticate two messages (one at a time) using only three subkeys of length p in total instead of four. (which would be required if we used independent key to authenticate each message). Show an explicit attack on one of the schemes.

i) $Dave$: $mac_1(m_1, k_1, k_2, k_3) := m_1 \cdot k_1 + k_2 \qquad mac_2(m_2, k_1, k_2, k_3) := m_1 \cdot k_1 + k_3$

ii) $Evan$: $mac_1(m_1, k_1, k_2, k_3) := m_1 \cdot k_1 + k_2 \qquad mac_2(m_2, k_1, k_2, k_3) := m_1 \cdot k_3 + k_2$

Bonus:

i) Define security for this two-time mac

ii) Prove one of the schemes secure under the two-time mac

8) Generalise the secure scheme in question 6 to d messages

9) Explain the relationship between enigma's weakness and exercise 2.7

Book exercises 1.1, 1.2, 1,5, 1.6, 2.3, 2.6, 2.7, 2.10, 2.13