CSCI361 Autumn 2015 exam Wollongong (Supplementary)

Database Management (Singapore Institute of Management)

UNIVERSITY OF WOLLONGONG
AUSTRALIA

School of Computing and Information Technology

Student to complete:

Family name	
Other names	
Student number	
Table number	

CSCI361
Cryptography and Secure Applications
Wollongong Campus

Supplementary Examination Paper
Autumn Session 2015

Exam duration	3 hours
Items permitted by examiner	UOW Approved Calculator
Aids supplied	Nil
Directions to students	Write all your answers in the examination booklet provided

Clearly mark the question numbers

Start each of the two sections on a new page

Satisfactory performance in this supplementary exam will allow students to obtain a 50-PS in this subject, otherwise an F or TF grade will be received.

This exam paper must not be removed from the exam venue

Section I: Modern and Classical Symmetric Key Cryptology (20 marks)

1. Consider a block cipher which has 3 rounds of encryption using the Feistel structure. The block has an 8 bit block size, a 6 bit key $\mathbf{k_1k_2k_3k_4k_5k_6}$, and uses an **f**-function. The cipher details are as follows:
   - The round keys for rounds 1, 2 and 3 are, respectively, $\mathbf{k_1k_3k_4k_2}$, $\mathbf{k_2k_4k_5k_3}$, and $\mathbf{k_3k_5k_6k_4}$.
   - The **f**-function works as follows:
     1. It takes a 4 bit input **X** and 4 bit key **K**.
     2. Determines and outputs the 4 bit string **Y = X*K mod 16**, based on the integer values of **X** and **K**.

   (i) Sketch a diagram for the encryption algorithm, showing where round keys and round inputs are used. Explain all notation used. (**2 marks**)

   (ii) Find the cryptogram for the key **110010** and the message **10101101**. Specify all round keys being used in the calculations, and give all the intermediate values of the encryption algorithm (after each round). (**4 marks**)

2. Decrypt the following ciphertext which was generated using the subsequently defined product cipher. (**4 marks**)

   VDAAPARAYGYGFTCNQJCNQTRNVYCQFCGFQKVQNFCCQJTTGNXR

   a. The plaintext was firstly processed through an array based transposition block cipher of length 24 letters, with key **435162**.

   b. To the results of the first part apply a shift cipher with a key corresponding to one less than that for the classical Caesar cipher.

   You should add spaces back into the message as best you can.

3. Explain the terms unbroken and secure in the context of computational security. (**2 marks**)

4. Consider that you have a cipher and key with the following mapping.

Input	000	001	010	011	100	101	110	111
Output	010	100	011	001	110	000	101	111

   (i) Describe the purpose of a mode. (**0.5 mark**)

   (ii) Describe CBC mode in general, carefully explaining the notation used. (**1 mark**)

   (iii) Encrypt the plaintext 101101110010 using this cipher in CBC mode. (**1.5 marks**)

5. In the context of DES, what does it mean for a key to be weak? (**1 mark**)

6. What are S-boxes, where are they used, and what purpose do they serve? **(1 mark)**

7. Give an example of an affine cipher that illustrates the need to avoid key values that result in ambiguous ciphertext. Illustrate such ambiguity. **(2 marks)**

8. Briefly describe the difference between pre-image resistance and second pre-image resistance. **(1 mark)**

Section II: Public Key Cryptography and Secure Applications **(10 marks)**

1. What are the differences between a Message Authentication Code (MAC) and a digital signature? **(1 mark)**

2. Describe the ElGamal encryption scheme, including key generation, encryption, and decryption. **(3 marks)**

3. Describe the Diffie-Hellman Key Exchange protocol, and the hard problem the protocol is based on. **(3 marks)**

4. What are the two basic security requirements of a commitment scheme? **(2 marks)**

5. Describe the homomorphic property of Shamir's Secret Sharing Scheme. **(1 mark)**

~ END OF EXAMINATION ~