CSCI361 Autumn 2015 exam Wollongong

System Administration (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

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 section on a new page This paper is worth 60% of the total marks for the subject

This exam paper must not be removed from the exam venue

Section I: Foundations and Classical Cryptology (15 marks)

1. Name and describe the three fundamental security properties. **(2 marks)**

2. Explain the terms broken and insecure in the context of computational security. **(2 marks)**

3. Consider the following ciphertext, generated from ordinary English text using a monoalphabetic substitution cipher:

YKHLBA JCZ SVIJ JZB TZVHI JCZ VHJ DR IZXKHLBA VSS RDHEI DR YVJV
LBXSKYLBA YLALJVS IFZZXC CVI LEFHDNZY EVBLRDSY JCZ FHLEVHT
HZVIDB RDH JCLI CVI WZZB JCZ VYNZBJ DR ELXHDZSZXJHDBLXI JCZ
XDEFSZQLJT DR JCZ RKBXJLDBI JCVJ XVB BDP WZ FZHRDHEZY WT JCZ
EVXCLBZ CVI HLIZB YHVEVJLXVSST VI V HZIKSJ DR JCLI HZXZBJ
YZNZSDFEZBJ LB JZXCBDSDAT EVBT DR JCZ XLFCZH ITIJZEI JCVJ
PZHZ DBXZ XDBILYZHZY IZXKHZ VHZ BDP WHZVMVWSZ.

(i) Describe two pieces of evidence you could use to convince someone that this ciphertext was generated using a monoalphabetic substitution cipher? **(1 mark)**

(ii) Describe four steps you could take to cryptanalyse this ciphertext. For at least two of those steps you should make specific reference to the ciphertext above. **(2 marks)**

4. Briefly describe the form of a homophonic substitution cipher and explain the reason for considering such a cipher. **(2 marks)**

5. 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)**

6. 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.

Section II: Modern Symmetric Key Cryptosystems (15 marks)

1. How is the principle of timeliness linked to the choice of key sizes? (**1 mark**)

2. 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 $k_1k_2k_3k_4k_5k_6$, and uses an f-function. The cipher details are as follows:
   - The round keys for rounds 1, 2 and 3 are, respectively, $k_1k_3k_4k_2$, $k_2k_4k_5k_3$, and $k_3k_5k_6k_4$.
   - 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**)

3. Briefly describe the following properties in the context of hash functions.

   (i) Pre-image resistance. (**1 mark**)

   (ii) Collision resistance. (**1 mark**)

4. A product cipher built by performing encryption under k_1 followed by performing encryption under k_2, as in double DES, is vulnerable to a meet-in-the-middle attack. Describe this attack and determine the effective overall key size, assuming k_1 and k_2 are arbitrary n-bit keys. (**3 marks**)

5. Describe Electronic Codebook mode and Counter mode for a block cipher. Give one advantage of each, and a disadvantage of one of them. (**2 marks**)

6. Briefly describe the concept of diffusion. (**1 mark**)

Section III: Public Key Cryptosystem (15 marks)

1. Describe two advantages of public key cryptosystems compared with symmetric key systems. (**2 marks**)

2. Calculate the GCD of 19 and 23, and the inverse of 19 mod 23. (**2 marks**)

3. Calculate 5^{97} mod 29. (**2 marks**)

4. Alice chooses two primes p = 13 and q = 17 as the first step in the generation of her key pair for the RSA cryptosystem. Complete the process by generating a pair of public and private key for Alice. **(3 marks)**

5. Show that if Bob can solve the factorisation problem, then Bob can break the RSA cryptosystem. **(1 mark)**

6. Consider the Digital Signature Algorithm (DSA) you have studied in the lecture

   Parameters: a large prime p, a prime divisor q of (p-1), a generator g of order q.
   Secret key: $0 < x < q$
   Public key: $g^x \bmod p$
   Sign a message M:
   a. Randomly choose $0 < k < q$
   b. $r = (g^k \bmod p) \bmod q$
   c. $s = (k^{-1}(H(M) + xr)) \bmod q$
   d. Return the signature as (r, s)

   (i) Describe the verification algorithm. **(1 mark)**
   (ii) In order to save some computation, Alice decided to use the same random number k to sign two different messages M1 and M2. Will this cause any problem? Justify your answer. **(2 marks)**

7. Describe the Diffie-Hellman key exchange protocol. Is the protocol secure under active attacks? Justify your answer. **(2 marks)**

Section IV: Security Applications (15 marks)

1. What are the security requirements of an e-voting system? **(2 marks)**

2. What is a blind signature? Describe one example of it. **(4 marks)**

3. Describe the structure of a mix-net. You can draw a diagram to assist your answer. **(3 marks)**

4. Describe one of the solutions you have learnt in the lecture to do Optimistic Fair Exchange of two digital signatures. **(2 marks)**

5. Alice, Bob and Carl have the following problem. They want to know the sum of their money, but they do not want to reveal their individual amount to each other. Design a secure protocol that can solve this problem. You can assume that there is no collusion between any two of the three parties. **(4 marks)**

~ END OF EXAMINATION ~