School of Computing and Information Technology

Student to complete:

Family name	
Other names	
Student number	

CSCI361
Cryptography and Secure Applications
CCCU Hong Kong Campus

Examination Paper
Semester C 2019/2020

Instructions

• Total marks: 100
• Duration for this is exam is 4 hours.
• No extension will be given. Allow enough time to upload your answer file before the exam period ends.
• You must not consult any material other than lecture slides and workshop notes.
• You are permitted to use a scientific calculator.
• You must not consult anyone.
• You must not collaborate with your peers.
• Your answers may be examined further for possible violations of the above three rules. If the offence is detected, you will get 0 for your final examination.

• Submission method:
1. For non-programming questions: students type or scan all your answer in one word or pdf file, CSCI361_answerbook_<your_name>_<your_studentID>.doc or pdf.

2. For programming questions: capture your demo screen and submit your source code.

3. Make sure that the answer file is one zip file, CSCI361_<your_name>_<your _studentID>.zip.

This study source was downloaded by 100000806118722 from CourseHero.com on 12-31-2024 19:43:50 GMT -06:00

https://www.coursehero.com/file/99795509/CSCI361-SemC2020-Exam-HKCCCU-online-final-assessment-29-julypdf/

4. Upload your answer file to the Moodle Final Examination section.

Part A: Math Computations **(Total 9 Marks)**

Answer all questions in this part
Explain your answer step-by-step. Answers without justification will gain no mark.

The value of x is your UOW student ID

1. GCD(x, 2020) 3 marks

2. x^{-1} (mod 97) 3 marks

3. 6^x mod 37 3 marks

Part B: Cryptographic Schemes and Applications (Total 91 Marks)

Answer all questions in this part

1. Decrypt the ciphertext "ohduq pruh", which is generated by a Caesar cipher. 1 mark
2. Encrypt the message "competition" using the key "exam" in a Vigenere cipher. 2 marks

3. Consider the following simple block cipher with block size 3.

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

Given a plaintext 111101111, compute the corresponding ciphertext for each of the following modes:

a. ECB 2 marks

b. CBC with IV = 000 3 marks

c. Counter with IV = 111 3 marks

This study source was downloaded by 100000806118722 from CourseHero.com on 12-31-2024 19:43:50 GMT -06:00

https://www.coursehero.com/file/99795509/CSCI361-SemC2020-Exam-HKCCCU-online-final-assessment-29-julypdf/

4. 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**.

      a. Sketch a diagram for the encryption algorithm, showing where round keys and round inputs are used. Explain all notation used.

      4 marks

      b. 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).

      9 marks

5. Consider the RSA encryption scheme, **Alice wants to send a message to Bob**. Both Alice and Bob have p = 17, q = 19. Alice has e=31 and Bob has e=29.
   a. What is the public key pair used in the transmission? 2 marks

   b. What is the secret key pair used in the transmission? 4 marks

   c. Encrypt the message m=111. 4 marks

   d. Decrypt the resulting ciphertext. 4 marks

   e. What's the security problem between Alice and Bob? How to solve this problem. Explain your answer. 3 marks

6. Consider the ElGamal encryption you have studied in the lecture.
   Parameters: a prime p, a generator g, a random number u, let $y = g^u \bmod p$.
   Public key: p, g, y
   Secret key: p, g, u
   Encryption of message M:
   - Choose a random number k<p-1
   - Let $a = g^k \bmod p$, $b = M\, y^k \bmod p$.
   - The ciphertext is (a,b)

   a. Describe the decryption algorithm. 2 marks

   b. Suppose p = 13, u = 4, g=2, k=3.

This study source was downloaded by 100000806118722 from CourseHero.com on 12-31-2024 19:43:50 GMT -06:00

https://www.coursehero.com/file/99795509/CSCI361-SemC2020-Exam-HKCCCU-online-final-assessment-29-julypdf/

i. What are the public key and secret key? 3 marks

ii. Encrypt the message M = 7. 4 marks

iii. Decrypt the corresponding ciphertext. 3 marks

c. Write a program by using PARI/PG to encrypt any message. 15 marks

To implement a GP program, which is called 'elgamal.gp'. The program must have the following function:

- KeyGen(p): a function to produce public key and secret key
- Encrypt(m): a function to encrypt the message.

7. a. Consider the (3,5)-secret sharing scheme due to Shamir working in Z_{11}. Suppose 7 is the secret. Show how the secret can be shared amongst 5 participants and how to reconstruct the secret from secret shares. 8 marks

b. Write a program by using PARI/PG to implement Shamir secret sharing. 15 marks

To implement a GP program, which is called 'sss.gp'. The program must have the following function:

- SecretShare (k,n,s,p): in the field Z_p, n is the total number of participants, k is the number of participants to reconstruct the secret, s is the secret
- Reconstruct ($[x_1,x_2,..x_k]$,$[s_1,s_2,..s_k]$,p): in the field Z_p, a function to recover the secret from k shares.

End of Examination

This study source was downloaded by 100000806118722 from CourseHero.com on 12-31-2024 19:43:50 GMT -06:00

https://www.coursehero.com/file/99795509/CSCI361-SemC2020-Exam-HKCCCU-online-final-assessment-29-julypdf/