Sample Exam
COMP6453

Monday 12 August 2024

Maximum Marks: 100

If you have not used the CSE lab machines this term, we strongly recommend that you familiarise yourself with the lab machines before the day of the exam by coming in to the lab.

Exam Rules and Conditions

Please read these rules carefully. Note that deliberate violation of exam conditions will be referred to Student Integrity as serious misconduct.

Duration

- There will be 10 minutes of reading time. You can start reading when your supervisor tells you to do so.
- Your supervisor will tell you when you can start working.
- You have 3 hours* to work on the exam. You must stop working once your supervisor tells you to do so.
- * Students with extra exam time approved by Equitable Learning Services (ELS) will be given extra time to complete the exam [illegible]

Communication

- You are not permitte[illegible] exam supervisors.
- If you have any quest[illegible] upervisor.

Resources

- The Internet will be [illegible] access the files in your normal CSE account. [illegible]
- You have been provid[illegible] any of these resources in your own answers. [illegible]

Special Consideratio[illegible]

- By starting this exam [illegible] annot apply for Special Consideration for issu[illegible]
- If a circumstance aris[illegible] exam, please raise your hand and talk to a su[illegible] mediately and apply for special consideration [illegible]

Submission

- See the submission instructions under each question.
- You can submit multiple times. Only your last submission will be marked.
- Do not wait until just before the deadline to submit all your answers. Submit each question as soon as you finish working on it or submit incrementally throughout the exam.

Short-Answer Questions

- Justifications/explanations are only required when asked by the question.

Marking

- Partial marks will be given for correct approach to problems.

Admin

Marks	Contributes to
Total Marks	100
Total number of questions	8 (note: the real exam may have a different number of questions)

Question 1 (15 Marks)

Write your answers for this question in q1.txt.
Solve the following questions showing all the steps of computation.

(a) (3 Marks)

Compute $2^{20} \mod 13$

(b) (2 Marks)

Compute $gcd(123, 276)$

(c) (5 Marks)

Compute multiplicative Inverse of 357 mod 1234

(d) (5 Marks)

Solve the following sy

Question 2 (10 Marks)

Write your answers for
For shift, mono-alphabe

(a) (3 Marks)

Prove that if only a s y secret.

(b) (5 marks)

What is the largest m cipher provides perfect secrecy?

(c) (2 Marks)

Prove that the Vigene to encrypt messages of length t.

Question 3 (10 Marks)

Write your answers for this question in q3.txt.

Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

Question 4 (20 Marks)

Write your answers for this question in q4.txt.

(a) (3 Marks) What are the challenges in storing data in untrusted servers, for example clouds?

(b) (10 Marks) I have stored a large file F in an untrusted server. I do not have a local copy on my disk. How can I verify the integrity of F without downloading the whole file?

(c) (7 Marks) What is the communication and computation complexity of the procedure?

Question 5 (10 Marks)

Write your answers for this question in q5.txt. Consider the following key-exchange protocol:

1. Alice chooses uniform $k, r \in \{0,1\}^n$, and sends $s := k \oplus r$ to Bob.
2. Bob chooses uniform $t \in \{0,1\}^n$, and sends $u := s \oplus t$ to Alice.
3. Alice computes $w := u \oplus r$ and sends w to Bob.
4. Alice outputs k and Bob outputs $w \oplus t$.

Answer the following two questions:

(a) (5 Marks)

Show that Alice and Bob output the same key.

(b) (5 Marks)

Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

Question 6 (10 Marks)

Write your answers for

Consider the Protocol b .

Each user U will have a ication algorithm ver_U. The TA also has a signatu user U has a certificate $Cert(U) = (ID(U), ver_U, s$

(a) (7 Marks)

Show how this protoc

(b) (3 Marks)

Discuss the conseque ties and how they are violated.

The public domain parame rder n.

1. U chooses a random

and she sends $Cert(U)$

2. V chooses a random

$$b_V = \alpha^{a_V}$$

$$K = (b_U)^{a_V},$$

and

$$y_V = sig_V(b_V||b_U).$$

Then V sends $Cert(V)$ (Certificate for V), b_V and y_V to U.

3. U verifies y_V using ver_V. If the signature y_V is not valid, then she “rejects” and quits. Otherwise, she “accepts,” she computes

$$K = (b_V)a_U,$$

and

$$y_U = sig_U(b_U||b_V),$$

and she sends y_U to V.

4. V verifies y_U using ver_U. If the signature y_U is not valid, then he “rejects”; otherwise, he “accepts.”

Question 7 (10 Marks)

Write your answers for this question in q7.txt.

Given two graphs G_0 and G_1, Prover P wants to convince verifier V that it knows a permutation π such that $\pi(G_0) = G_1$. P could simply send π to V, but that is hardly zero-knowledge; we want to convince V that π is an isomorphism without revealing anything about it. The protocol is as follows:

$P \to V$: P randomly chooses a permutation σ and a bit $b \in \{0,1\}$, computes $H = \sigma(G_b)$, and sends H to V.

$V \to P$: V chooses a bit $b_0 \overset{R}{\leftarrow} \{0,1\}$ and sends it to P.

$P \to V$: P sends the permutation τ to V , where

$$\tau = \begin{cases} \sigma & b = b' \\ \sigma\pi^{-1} & b = 0, b' = 1 \\ \sigma\pi & b = 1, b' = 0 \end{cases}$$

V accepts if and only if $H = \tau(G_{b_0})$ and τ is a one-to-one mapping between vertices and edges.

(a) (5 Marks)

Complete

(b) (5 Marks)

Sound and

(c) (5 Marks)

Zero-knowledge.

Question 8 (15 Marks)

Write your answers for

Data from N communi gregator node n_a. The aggregator node has to veri

(a) (3 Marks)

How can you do so us

(b) (4 Marks)

What is the complexi

(c) (4 Marks)

Can you design an efficient algorithm to reduce the verification time?

(d) (4 Marks)

What is the new time complexity of the new verification algorithm?

Wish you all the best!