COMP3335 Database Security

Semester 1, 2023/2024

October 4, 2023

~~10~~ 9

Student ID: 21093962D Student Name: JIANG Guanlin

Quiz 1

This is a closed-book exam. Complete your ID and name above first. When instructed, open the booklet and answer the multiple choice questions by **circling** the right answer (there is only one possible correct answer per question). Continue by answering questions in the spaces provided. If you run out of room for an answer, it is most likely getting too long. As a reminder, plagiarism is a serious offence. If you are caught cheating, you will first get a warning; if repeated, you will be dismissed and receive a zero for this quiz. If you finish the quiz and there is less than 10 minutes remaining, stay until the end.

Total: 12 points worth 12% of the course weight. Total pages: 3

Allowed time: 40 minutes

1. The equivalent of SQL tables in NoSQL database systems is called: (0.5 pt)
   A. Columns
   B. Collections
   C. Documents
   D. Records

2. Which process helps to normalize a SQL table? (0.5 pt)
   A. Horizontal data fragmentation
   B. Data allocation
   C. Functional dependency analysis
   D. Sharding

3. Which of the following is an example of a relational database management system (RDBMS)? (0.5 pt)
   A. MongoDB
   B. Oracle
   C. Redis
   D. Neo4j

4. Which of the following cryptographic algorithms is preferred nowadays for hashing? (0.5 pt)
   A. DES
   B. AES
   C. SHA1
   D. SHA256

5. In database security, what does the term "integrity" refer to? (0.5 pt)
   A. Keeping data private
   B. Ensuring data is up-to-date
   C. Ensuring data is accurate and unchanged from its original form
   D. Keeping the database available at all times

6. In horizontal fragmentation, records of a table are divided among different locations based on: (0.5 pt)
   A. Their columns
   B. The preference of the user whose data is in the table
   C. The order in which they were added
   D. Certain conditions, ranges specified on one or more columns, or evenly distributed

7. Explain the differences between symmetric and asymmetric encryption. (1 pt)

symmetric encryption use a key secert (password) to encryt the content or data.
Asymmetric encryption use the private key and public key to encryt, only can use private key to decrypt.

8. What are the three main requirements on information security? (1 pt)

availability, confidentiality, integrity.

9. Which information security requirement may involve encryption as a solution? (1 pt)

confidentiality will be involve.
Cryptographic hashing and encryption

10. Explain the mutual consistency rule. (1 pt)

The mutual consistency rule is the data must be same after write, so the user can read the data, need some time to copy the data.

11. Explain the CAP theorem. (1 pt)

The CAP theorem is the availability, confidentiality, and fault tolerance only can satisfy 2/3.
The CAP theorem is a distributed database has to make a tradeoff between Consistency and availability when a partition occurs.

12. In MongoDB, if a replica set has 7 members, what is the fault tolerance? (1 pt)

the fault tolerance is 3.

13. Consider the table `real_estate` below as we discussed in class and answer the following questions.

Realtor Name	Office Address	Office City	Realtor Phone	Property Address	Property City	Beds	Area	Price
Penny	137 Main	CityA	555-1111	17 Highland	CityA	3	2000	220000
Penny	137 Main	CityA	555-1111	1565 State Rd	CityB	4	2900	290000
Penny	137 Main	CityA	555-1111	997 George	CityA	4	2200	240000
Penny	137 Main	CityA	555-1111	123 Big Lane	CityA	8	5000	750000
Bob	455 Oak	CityB	555-2222	5 Lighthouse	CityB	4	2000	230000
Bob	455 Oak	CityB	555-2222	190 Brown	CityC	2	1700	140000
Bob	455 Oak	CityB	555-2222	123 Big Lane	CityA	8	5000	750000

a. Identify <u>one</u> functional dependency in this table. (1.5 pts)

office City can be functional dependency.
Property City + Realtor Number → Property Address → Beds

b. What does the following SQL command do in MySQL 8.0? (1.5 pts)

```
ALTER TABLE real_estate PARTITION BY HASH(`Office_Address`) PARTITIONS 4;
```

this command let the table real_estate spilt to 4 data files by the different office address which after hashing.