**ĐỀ CƯƠNG ÔN TẬP**

HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

-------------------

**“AN TOÀN CƠ SỞ DỮ LIỆU”**

*Giảng viên: Trần Thị Lượng*

**Chương 1: Tổng quan về an toàn thông tin trong CSDL**

1. Các mối đe dọa, các tấn công có thể đến với CSDL là gì?

2. Tìm hiểu các cấu hình xử lý CSDL (CSDL tập trung, phân tán, Client/Server). Các cấu hình này được áp dụng như thế nào trong thực tế. (Chú ý: nêu rõ đặc điểm – bản chất và vẽ hình minh họa).

3. Các bước để thiết kế cơ sở dữ liệu (mô tả). Học và viết được (chính xác) những câu lệnh SQL cơ bản trong quá trình thiết kế CSDL.

4. Khi cần thiết kế một CSDL an toàn phải đưa ra được các giải pháp an toàn cho bài toán đó gắn với hệ quản trị cụ thể.

5. Trình bày về SQL, các câu lệnh SQL cơ bản.

6. Trình bày các yêu cầu bảo vệ CSDL .

7. Trình bày một số phương pháp (được tích hợp sẵn trong các DBMS) để đảm bảo tính toàn vẹn dữ liệu.

8. Tìm hiểu về Transaction và quá trình thực hiện một Transaction.

9. Tìm hiểu những vấn đề cần thiết khi mã hóa CSDL (vấn đề mã hóa ở đâu, bảo vệ khóa, phân phối khóa như thế nào…)

**Chương 2. Các mô hình và chính sách an toàn**

1. Nêu rõ đặc điểm của kiểm soát truy nhập MAC và DAC trong CSDL, nêu sự khác nhau giữa chúng. Ứng dụng 2 chính sách này trong thực tế các hệ quản trị như thế nào?

Trình bày về hệ thống Multilevel security: đ/n, các đặc điểm chính, ví dụ.

2. Thế nào là mô hình an toàn? Sự khác nhau giữa mô hình an toàn và chính sách an toàn. Tìm hiểu mô hình an toàn là Bell-Lapadula.

3. Trình bày cơ bản về một số phương pháp có thể bảo vệ CSDL trong hệ quản trị Oracle (chẳng hạn: VPD, mã hóa CSDL, OLS, Kiểm toán…), các phương pháp đảm bảo tính toàn vẹn CSDL trong DBMS.

4. Trình bày những lớp người dùng chính của một hệ thống an toàn CSDL và vai trò của họ.

5. Trình bày việc gán/thu hồi quyền trong MAC và DAC.

6. Trình bày đặc điểm cơ bản về mô hình RBAC.

7. Tìm hiểu mô hình cấp quyền System R. Đặc biệt lưu ý vấn đề thu hồi quyền đệ quy và không đệ quy.

1. Nêu ví dụ về đặc quyền hệ thống (System Prilvilege) và đặc quyền đối tượng (Object Prilvilege), viết câu lệnh SQL cho các ví dụ đó. Nêu sự khác nhau giữa Admin option và Grant option. (Ví dụ các câu lệnh SQL).

**Chương 3.**

Tìm hiểu đặc điểm cơ bản của kiến trúc chủ thể tin cậy (Trusted Subject) và kiến trúc Integrity Lock. Đặc biệt chú ý kiến trúc Intergrity Lock (cả lý thuyết và bài tập).

**Chương 4.**

Tìm hiểu kỹ về khái niệm và ý tưởng của tấn công SQL Injection

**Chương 5 Cơ sở dữ liệu thống kê**

1. Cơ sở dữ liệu thống kê (statistical database) là gì? (Viết được các câu lệnh SQL cho các thống kê). Ứng dụng trong thực tế? Các dạng biểu diễn.
2. Tìm hiểu những khái niệm cơ bản trong CSDL thống kê.
3. Thế nào là thống kê nhạy cảm, cho ví dụ? Working knowledge và Supplementary knowledge?
4. Nêu đặc điểm cơ bản về Tấn công dựa vào Trình theo dõi (trình bày được ý tưởng của 2 kiểu tấn công này) và cho ví dụ.
5. Tìm hiểu các kỹ thuật chống suy diễn trong CSDL thống kê, nêu ưu nhược điểm của từng phương pháp. (Chú ý tìm hiểu kỹ các kiểm soát này)
   * Kiểm soát kích cỡ tập truy vấn
   * Kỹ thuật giấu ô
   * Kỹ thuật gây nhiễu

**BÀI TẬP:**

Lưu ý một số dạng bài tập sau:

* Bài tập thiết kế CSDL
* Bài tập chương 5 về tấn công suy diễn và kỹ thuật giấu ô
* Bài tập chương 3 về Gắn tem, giải thích tại sao đảm bảo được tính toàn vẹn cho CSDL bằng kỹ thuật Intergrity Lock
* Bài tập về Multilevel Security + Bellapadula.
* Đề thi có thể có một vài ý nhỏ mở rộng ko nằm trong đề cương.

**LƯU Ý:**

* + **Sinh viên cần nắm rõ các câu lệnh SQL để minh họa cho các phần đã đề cập, ngoài ra mỗi phần có thể cần hình vẽ để minh họa.**
  + **Đề thi không được sử dụng tài liệu**
  + **Nếu sinh viên chép bài của nhau đều bị 0 điểm.**