COURSE SYLLABUS  
**<Course ID> – <Course Name>**

# GENERAL INFORMATION

|  |  |
| --- | --- |
| Course name: | Database Security |
| Course name (in Vietnamese): | Bảo mật Cơ sở Dữ liệu |
| Course ID: | CSC15002 |
| Knowledge block: | Specialty |
| Number of credits: | 4 |
| Credit hours for theory: | 45 |
| Credit hours for practice: | 30 |
| Credit hours for self-study: | 90 |
| Prerequisite: | Introduction to Cryptography/Applied cryptography |
| Prior-course: | Introduction to Database |
| Instructors: | Nguyen Dinh Thuc – Tran Ngoc Bao |

# COURSE DESCRIPTION

The course aims to help students understand and apply encryption and information security methods for designing and protecting an information system. Specifically, can understand and apply access control methods, traditional as well as modern database security methods. In addition, students can apply skills such as teamwork, can read English documents. In addition, in terms of attitude, students know about professional ethics and responsibility

# COURSE GOALS

At the end of the course, students are able to

|  |  |  |
| --- | --- | --- |
| **ID** | **Description** | **Program LOs** |
| G1 | Team work skills  Reading and reporting skills |  |
| G2 | Know critical thinking, professional ethics, and responsibility. |  |
| G3 | Can use access control mechanisms provided by DBMS |  |
| G4 | Understand and can apply encryption methods for database security. |  |

# COURSE OUTCOMES

|  |  |  |
| --- | --- | --- |
| **CO** | **Description** | **I/T/U** |
| G1.1 | Team work skill | U |
| G1.2 | Know and understand specialized English terms of the subject | U |
| G1.3 | Writing and speaking skills, presentation skills (in Vietnamese) related to subject topics. | I, U |
| G2.1 | Cultural knowledge, professional ethics, responsibility and regulatory aspects related to topics in the subject. | U |
| G3.1 | Understand database access control mechanisms | T, U |
| G3.2 | Can use database access control mechanisms | T, U |
| G4.1 | Understand encryption algorithms, tools | T, U |
| G4.2 | Can use database encryption techniques | T, U |
| G4.3 | Understand and can design a database for security tasks | I, T |

# TEACHING PLAN

**THEORY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Topic** | **Course outcomes** | **Teaching/Learning Activities (samples)** | **Assessments** |
| 1 | Introduction to database security | G1  G2 | Lecturing | HW1 |
| 2 | Applied cryptography | G2.  G4.1 | Lecturing  Demonstration, Q&A | HW2 |
| 3 | Crypto systems | G2  G4.1, G4.2 | Lecturing  Demonstration, Q&A and discussion | HW3 |
| 4 | Homomorphic cryptosystems and database security | G2  G4.1, G4.2 | Lecturing  Demonstration, Q&A and discussion | HW4 |
| 5 | Cryptographic hash functions and database security | G2  G4.1, G4.2 | Lecturing  Demonstration, Q&A and discussion | HW5 |
| 6 | Database security: classical methods (CRT-based content protection) | G4.1, G4.2 | Lecturing  Demonstration, Q&A and discussion | HW6 |
| 7 | Database security: cryptography-based methods (secure index 1) | G4.1, G4.2 | Lecturing  Demonstration, Q&A and discussion | HW7 |
| 8 | Database security: cryptography-based methods (secure index 2) |  | Lecturing  Demonstration, Q&A and discussion | HW7 |
| 9 | Database design for database security | 4.2, 4.3 | Example-based teaching (Interactive teaching) | HW8 |
| 10 | Application models | 3  4 | Lecturing  Demonstration, Q&A and discussion | HW9 |
| 11 | Review |  | Lecturing  Q&A, Discussion |  |

**LABORATORY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Topic** | **Course outcomes** | **Teaching/Learning Activities (samples)** | **Assessments** |
| 1 | Install a DBMS with security-options | G1  G2 | Explain and demonstrate  Q&A, Group discussion | LW1  (individual project and 2-persons group project ) |
| 2 | Using security functions/tools that DBMS provides | G1  G2 | Lecturing  Demonstration, Q&A | LW2  (individual project and 2-persons group project ) |
| 3 | Database access control | G2  G3 | Provide instructions  Demonstration, discussion | LW3  (individual project and 2-persons group project ) |
| 4 | Database encryption | G3 | Lecturing  Demonstration, discussion | LW4  (individual project and 2-persons group project ) |
| 5 | Database design for database security | G4 | Lecturing  Demonstration | LW5  (individual project and 2-persons group project ) |

# ASSESSMENTS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Topic** | **Description** | **Course outcomes** | **Ratio (%)** |
| **A1** | **Assignments** |  |  | **20%** |
| A11 | Homework (HW1-HW100) | practicing based on knowledge taught in class |  | 20% |
| **A2** | **Projects** |  |  | **60%** |
| A21 | Individual Project |  |  | 30% |
| A22 | Group Project |  |  | 30% |
| **A3** | **Exams** |  |  | **20%** |
| A31 | Final oral exam | In-class programming exam on computer |  | 20% |

# RESOURCES

# Textbooks

* Bùi Doãn Khanh - Nguyễn Đình Thúc, Mã hoá Thông tin: Lý thuyết và Ứng dụng, NXBLĐXH, 2004.
* Jeffrey Hoffstein – Jill Pipher – Joseph H. Silverman, An introduction to mathematical cryptography, Springer, 2008.

# Others

* Papers (lecturer provides)

# GENERAL REGULATIONS & POLICIES

* All students are responsible for reading and following strictly the regulations and policies of the school and university.
* Students who are absent for more than 3 theory sessions are not allowed to take the exams.
* For any kind of cheating and plagiarism, students will be graded 0 for the course. The incident is then submitted to the school and university for further review.
* Students are encouraged to form study groups to discuss on the topics. However, individual work must be done and submitted on your own.